

Fermat's Last Theorem and Related Problems

Darrell Cox

January 17, 2018

Abstract

Empirical evidence in support of variants of Fermat's Last Theorem is presented.

1 Introduction

Let a , b , and c be natural numbers relatively prime in pairs and let p be an odd prime. Every prime factor of $(a^p + b^p)/(a + b)$ other than p is of the form $pk + 1$. p (and no higher power of p) divides $(a^p + b^p)/(a + b)$ if and only if p divides $a + b$. Let q be a natural number. q will be said to be a p th power with respect to $(a^p + b^p)/(a + b)$ if $q^{(f-1)/p} \equiv 1 \pmod{f}$ for every prime factor f , $f \neq p$, of $(a^p + b^p)/(a + b)$. Let $[(a^p + b^p)/(a + b)]$ denote $(a^p + b^p)/(a + b)/p$ if p divides $a + b$, or $(a^p + b^p)/(a + b)$ otherwise. Similarly, let $[a + b]$ denote $(a + b)/p$ if p divides $a + b$, or $a + b$ otherwise. The following two conjectures are the main topic of this article;

- (1) If $p > 3$, there do not exist a and b such that $[(a^p + b^p)/(a + b)]$ is a p th power.
- (2) If $p > 3$, there do not exist a and b such that $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ does not divide a , b , $a - b$, or $a + b$, and a , b , $a - b$, or $[a + b]$ is a p th power.

If the first conjecture is true, there are no solutions of Fermat's equation $a^p + b^p = c^p$ (which, of course, is already known). The second conjecture encompasses the first case of Fermat's Last Theorem (where p does not divide abc). (In 1810, Barlow [1] proved that $a^p + b^p = c^p$ only if $[(a^p + b^p)/(a + b)]$ is a p th power.) Let T be a natural number. Since a , b , and T are not symmetrical in the equation $[(a^p + b^p)/(a + b)] = T^p$, it is not obvious how to apply the theory of elliptic curves to these problems. The " p th power w.r.t." concept and the identity $a^p + b^p = (a^p - b^p) + 2b^p$ play a central role in proving these conjectures. For example, if p divides $a + b$ and $(a^p + b^p)/(a + b)/p$ is a p th power, then $p(a + b)/2$ is a p th power w.r.t. $(a^p - b^p)/(a - b)$ (this is a succinct way of saying that $(p(a + b))^{(f-1)/p} \equiv 2^{(f-1)/p} \pmod{f}$ for every prime factor f , $f \neq p$, of $(a^p - b^p)/(a - b)$). If p is not a p th power modulo a prime f of the form $pk + 1$,

then, for example, if f does not divide $a + b$, $(p^x(a + b))^{(f-1)/p} \equiv 1 \pmod{f}$, $0 \leq x < p$, has a solution (x defines a congruence class). Furthermore, if 2 is not a p th power modulo f , then, for example, $(2^y(a + b))^{(f-1)/p} \equiv 1 \pmod{f}$, $0 \leq y < p$, has a solution and $a + b$ can be eliminated from the congruences. The objective in the following is to eliminate a , b , $a - b$, and $a + b$ from certain congruences so that congruence relationships involving only 2 and p are obtained. When $p = 3$, there do exist a and b such that $[(a^p + b^p)/(a + b)]$ is a p th power and many properties of such a and b , among them reformulated versions of the classical Furtwängler and Vandiver theorems for Fermat's equation, can be empirically derived. In the following, these "propositions" are stated as if they were true for all p . One justification for doing this is the first conjecture above. Also, more properties of hypothetical solutions of Fermat's equation are shared by solutions of the equation $[(a^p + b^p)/(a + b)] = T^p$, $p = 3$. For example, it can be easily proved that $a^p + b^p = c^p$ implies 2 is a p th power w.r.t. $(a^p - b^p)/(a - b)$. Based on empirical evidence collected for $p = 3$, if $[(a^p + b^p)/(a + b)]$ is a p th power and $2p$ divides $a - b$ or $a + b$, then 2 is a p th power w.r.t. $(a^p - b^p)/(a - b)$ (although there is no apparent reason why this should be true).

2 Congruence Properties of Prime Factors of $[(a^p - b^p)/(a - b)]$ when $[(a^p + b^p)/(a + b)]$ is a p th Power

The following propositions are based on data collected for $p = 3$;

(3) If $[(a^p + b^p)/(a + b)]$ is a p th power and $2p$ does not divide a , b , $a - b$, or $a + b$, then 2, p , and $p/2$ are not p th powers w.r.t. $(a^p - b^p)/(a - b)$.

(4) If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ does not divide a , b , $a - b$, or $a + b$, and f is a prime factor of $[(a^p - b^p)/(a - b)]$, then 2 is a p th power modulo f if and only if f is of the form $p^2k + 1$.

By these two propositions, if $[(a^p + b^p)/(a + b)]$ is a p th power and $2p$ does not divide a , b , $a - b$, or $a + b$, then there is at least one prime factor of $[(a^p - b^p)/(a - b)]$ not of the form $p^2k + 1$. In 1912, Furtwängler [2] proved that if $a^p + b^p = c^p$, q divides a and p does not divide ac , or q divides b and p does not divide bc , then $q^{p-1} \equiv 1 \pmod{p^2}$. (Proofs of this theorem use the condition that $a + b$ must be a p th power and it is not obvious how to prove a reformulated version of the theorem without using this condition.) Furtwängler also proved that if $a^p + b^p = c^p$, q divides $a - b$ or $a + b$, and p does not divide $a - b$ or $a + b$, then $q^{p-1} \equiv 1 \pmod{p^2}$. Note that if p does not divide a natural number d , then $d^{p(p-1)} \equiv 1 \pmod{p^2}$ by Euler's theorem. Then if $q^{p-1} \equiv 1 \pmod{p^2}$, q is a p th power modulo p^2 . The reformulated version of Furtwängler's theorems is;

(5) If $[(a^p + b^p)/(a + b)]$ is a p th power and 2 does not divide a , then p does not divide a and every prime factor of a is a p th power modulo p^2 . If $[(a^p + b^p)/(a + b)]$ is a p th power, 2 divides a , and p does not divide a , then $(a/2)^{p-1} \equiv 1 \pmod{p^3}$. Analogous results hold for b . If $[(a^p + b^p)/(a + b)]$ is a p th power and 2 does not divide $a - b$, then p does not divide $a - b$ and every prime factor of $a - b$ is a p th power modulo p^2 . If $[(a^p + b^p)/(a + b)]$ is a p th power and 2 does not divide $a + b$, then p^2 does not divide $a + b$ and every prime factor of $a + b$ other than p (if p divides $a + b$) is a p th power modulo p^2 .

The peculiar form of Furtwängler's second theorem, that is, the condition that p not divide $a - b$ or $a + b$, makes sense when viewed from this perspective; 2 divides $a - b$ if and only if 2 divides $a + b$. This proposition implies that if $[(a^p + b^p)/(a + b)]$ is a p th power, p divides a , b , $a - b$, or $a + b$, and $2p$ does not divide a , b , $a - b$, or $a + b$, then 2 divides a or b , and p divides $a + b$. Note that this proposition implies "split" 2 and p are not possible when $a^p + b^p = c^p$, p divides c . (By Barlow's formulas, $p(a + b)$ must be a p th power when $a^p + b^p = c^p$, p divides c .) The requirement that $2p$ divide $a + b$ could be said to be a characteristic property of the equation $a^p + b^p = c^p$, p divides c . More propositions are;

(6) If $[(a^p + b^p)/(a + b)]$ is a p th power, then p^2 divides a if $2p$ divides a , p^2 divides b if $2p$ divides b , p^2 divides $a - b$ if $2p$ divides $a - b$, or p^3 divides $a + b$ if $2p$ divides $a + b$.

(7) If $[(a^p + b^p)/(a + b)]$ is a p th power, 2 divides a or b , and f is a prime factor of $[(a^p - b^p)/(a - b)]$ not of the form $p^2k + 1$, then exactly one of $2p$, p , or $p/2$ is a p th power modulo f .

(8) If $[(a^p + b^p)/(a + b)]$ is a p th power, p divides $a + b$, and f is a prime factor of $[(a^p - b^p)/(a - b)]$ of the form $p^2k + 1$, then pa , pb , $p^2(a - b)$, and $p(a + b)$ are p th powers modulo f . If $[(a^p + b^p)/(a + b)]$ is a p th power, p divides a , b , or $a - b$, and f is a prime factor of $[(a^p - b^p)/(a - b)]$ of the form $p^2k + 1$, then a , b , $p(a - b)$, and $a + b$ are p th powers modulo f .

Note that p is not precluded from being a p th power modulo f in Proposition (8). If $[(a^p + b^p)/(a + b)]$ is a p th power and $2p$ does not divide a , b , $a - b$, or $a + b$, there is apparently nothing to prevent p from being a p th power modulo every prime factor of $[(a^p - b^p)/(a - b)]$ not of the form $p^2k + 1$. By these propositions, if $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ does not divide a , b , $a - b$, or $a + b$, and p is a p th power modulo every prime factor of $[(a^p - b^p)/(a - b)]$ not of the form $p^2k + 1$, then a , b , $a - b$ and $[a + b]$ are not p th powers. (By Proposition (3), there would be at least one prime factor f of $[(a^p - b^p)/(a - b)]$ of the form $p^2k + 1$ such that p was not a p th power modulo f . Then by Proposition (8), a , b , $a - b$, or $[a + b]$ couldn't be a p th power.) More propositions are;

(9) If $[(a^p + b^p)/(a + b)]$ is a p th power, 2 divides a , p does not divide a , f is a prime factor of $[(a^p - b^p)/(a - b)]$ not of the form $p^2k + 1$, and $p/2$ is a p th

power modulo f , then pa , p^2b , $p(a-b)$, and $a+b$ are p th powers modulo f . If $[(a^p + b^p)/(a+b)]$ is a p th power, 2 divides a , p does not divide a , f is a prime factor of $[(a^p - b^p)/(a-b)]$ not of the form p^2k+1 , and $2p$ is a p th power modulo f , then pa , b , $a-b$, and $p^2(a+b)$ are p th powers modulo f . Analogous results hold for b .

(10) If $[(a^p + b^p)/(a+b)]$ is a p th power, 2 divides a , and p does not divide a , then pa , $2pb$, $2^2p^2(a-b)$, and $2^2p(a+b)$ are p th powers w.r.t. $(a^p - b^p)/(a-b)$. Also, either $2p$ is a p th power w.r.t. $(a^p - b^p)/(a-b)$ or none of $2p$, p , $p/2$, or 2 is a p th power w.r.t. $(a^p - b^p)/(a-b)$ (if $[(a^p - b^p)/(a-b)]$ has only one distinct prime factor, then $[(a^p - b^p)/(a-b)]$ is prime and $2p$ is a p th power w.r.t. $(a^p - b^p)/(a-b)$). Analogous results hold for b .

Note that if $2p$ is a p th power w.r.t. $(a^p - b^p)/(a-b)$ in Proposition (10), then $a/2$, b , $a-b$, and $[a+b]$ are p th powers w.r.t. $(a^p - b^p)/(a-b)$. Since Propositions (8), (9), and (10) are based solely on data collected for $p=3$, their form is sometimes ambiguous in that the p^2 and 2^2 factors might be p^{p-1} and 2^{p-1} instead. If $p(a+b)/2$ is a p th power w.r.t. $(a^p - b^p)/(a-b)$ (as implied by a second-case solution of Fermat's equation, p divides c , $p \geq 3$), f is a prime factor of $[(a^p - b^p)/(a-b)]$, and $2p$ is a p th power modulo f , then $p^2(a+b)$ is a p th power modulo f , so the p^2 factor of $a+b$ in Proposition (9) is unambiguous. Propositions (9) and (10) are consistent when p is not a p th power modulo f only if 8 is a p th power modulo f , but 8 can be a p th power modulo f only if $p=3$ ($2^{f-1} \equiv 1 \pmod{f}$) and $(2^3)^{(f-1)/p} \equiv 1 \pmod{f}$, $p \neq 3$, implies $2^{(f-1)/p} \equiv 1 \pmod{f}$ [since in this case, the greatest common divisor of $f-1$ and $3(f-1)/p$ is $(f-1)/p$], a contradiction. This follows from eliminating b , $a-b$, and $a+b$ from the congruences if 2 divides a , or eliminating a , $a-b$, and $a+b$ from the congruences if 2 divides b . If a $2^{p-1}p$ factor of the $a+b$ term in Proposition (10) had been used, some inconsistency for $p > 3$ could have been avoided (this implies $p/2$, 2^2p , and $2^{p-1}p$ are p th powers modulo f if $p/2$ is a p th power modulo f , or $2p$, 2^2p^2 , and $2^{p-1}/p$ are p th powers modulo f if $2p$ is a p th power modulo f). However, using a $2^{p-1}p^{p-1}$, 2^2p^{p-1} , $2^{p-1}p^2$, or 2^2p^2 factor of the $a-b$ term in Proposition (10) implies that 8 is a p th power modulo f , a contradiction for $p > 3$. This may just mean that one (or both) of the propositions is specific to $p=3$. It's plausible that the maximum p exponent used in Proposition (9) is related to the number of the terms a , b , $a-b$, and $a+b$ (and not to the p value itself). If p is not a p th power modulo f , then, for example, $(p^x(a-b))^{(f-1)/p} \equiv 1 \pmod{f}$, $0 \leq x < p$, has a solution, so Proposition (9) should remain the same for $p > 3$. If it's granted that $2p$ should be a p th power modulo f some of the time (note that this implies that p is not a p th power modulo f), then Proposition (10) should remain the same for $p > 3$. (In this case, eliminating b , $a-b$, and $a+b$ from the congruences if 2 divides a , or eliminating a , $a-b$, and $a+b$ from the congruences if 2 divides b , gives $2p$, 2^2p^2 , and $p/2^2$ are p th powers modulo f . Note that 2^2p^2 is the square of $2p$; $x=2$ is the only possible solution of $[2^x p^2(a-b)]^{(f-1)/p} \equiv 1 \pmod{f}$ when $x=1$ is the solution of $(2^x pa)^{(f-1)/p} \equiv 1 \pmod{f}$, 2 divides b , or $(2^x pb)^{(f-1)/p} \equiv 1 \pmod{f}$,

2 divides a). Other propositions are;

(11) If $[(a^p + b^p)/(a + b)]$ is a p th power, 2 divides a , f is a prime factor of $[(a^p - b^p)/(a - b)]$ not of the form $p^2k + 1$, and p is a p th power modulo f , then a , $2b$, $2^2(a - b)$, and $2^2(a + b)$ (and not 2) are p th powers modulo f . Analogous results hold for b . If $[(a^p + b^p)/(a + b)]$ is a p th power, 2 divides $a - b$ or $a + b$, f is a prime factor of $[(a^p - b^p)/(a - b)]$ not of the form $p^2k + 1$, and p is a p th power modulo f , then $a - b$, $a + b$, and 2 (and not a or b) are p th powers modulo f .

(12) If $[(a^p + b^p)/(a + b)]$ is a p th power, then a is a p th power w.r.t. $(a^p - b^p)/(a - b)$ if $2p$ divides a , or b is a p th power w.r.t. $(a^p - b^p)/(a - b)$ if $2p$ divides b , or $p(a - b)$ and $a + b$ are p th powers w.r.t. $(a^p - b^p)/(a - b)$ if $2p$ divides $a - b$, or $p^2(a - b)$ and $p(a + b)$ are p th powers w.r.t. $(a^p - b^p)/(a - b)$ if $2p$ divides $a + b$.

(13) If $[(a^p + b^p)/(a + b)]$ is a p th power and $2p$ divides $a - b$ or $a + b$, then 2 is a p th power w.r.t. $(a^p - b^p)/(a - b)$.

(14) If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides a , f is a prime factor of $[(a^p - b^p)/(a - b)]$ not of the form $p^2k + 1$, and $p/2$ is a p th power modulo f , then a , pb , $a - b$, and $p^2(a + b)$ are p th powers modulo f . If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides a , f is a prime factor of $[(a^p - b^p)/(a - b)]$ not of the form $p^2k + 1$, and $2p$ is a p th power modulo f , then a , p^2b , $p^2(a - b)$, and $p(a + b)$ are p th powers modulo f . Analogous results hold for b . If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides $a - b$, f is a prime factor of $[(a^p - b^p)/(a - b)]$ not of the form $p^2k + 1$, and p is not a p th power modulo f , then (1) pa , p^2b , $p(a - b)$, and $a + b$ are p th powers modulo f , or (2) p^2a , pb , $p(a - b)$, and $a + b$ are p th powers modulo f . If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides $a + b$, f is a prime factor of $[(a^p - b^p)/(a - b)]$ not of the form $p^2k + 1$, and p is not a p th power modulo f , then (1) a , p^2b , $p^2(a - b)$, and $p(a + b)$ are p th powers modulo f , or (2) p^2a , b , $p^2(a - b)$, and $p(a + b)$ are p th powers modulo f .

(15) If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides a or b , $[(a^p - b^p)/(a - b)]$ has two distinct prime factors, and neither distinct prime factor is of the form $p^2k + 1$, then $[(a^p - b^p)/(a - b)]$ is of the form $p^2k + 1$ and (1) $2p$ is a p th power modulo both distinct prime factors, or (2) p is a p th power modulo both distinct prime factors, or (3) $p/2$ is a p th power modulo both distinct prime factors. If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides $a - b$ or $a + b$, $[(a^p - b^p)/(a - b)]$ has two distinct prime factors, and neither distinct prime factor is of the form $p^2k + 1$, then $[(a^p - b^p)/(a - b)]$ is of the form $p^2k + 1$.

(16) If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides a , b , $a - b$, or $a + b$, and $2p$, $p/2$, or p (and not 2) is a p th power w.r.t. $(a^p - b^p)/(a - b)$, then p divides a or b and at least one prime factor of $[(a^p - b^p)/(a - b)]$ is not of the form $p^2k + 1$. If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides a , b , $a - b$, or $a + b$, and $[(a^p - b^p)/(a - b)]$ has only one distinct prime factor, then $2p$, $p/2$, or p is not a p th power w.r.t. $(a^p - b^p)/(a - b)$ when 2 is not a p th power w.r.t. $(a^p - b^p)/(a - b)$. If

$[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides a , b , $a - b$, or $a + b$, $[(a^p - b^p)/(a - b)]$ has exactly two distinct prime factors, $[(a^p - b^p)/(a - b)] \neq p_1^{k_1} p_2^{k_2}$ where p divides k_1 or k_2 , and $2p$, $p/2$, or p (and not 2) is a p th power w.r.t. $(a^p - b^p)/(a - b)$, then both distinct prime factors of $[(a^p - b^p)/(a - b)]$ are not of the form $p^2k + 1$.

In this section, it is assumed that $[(a^p - b^p)/(a - b)]$ can't be a p th power when $[(a^p + b^p)/(a + b)]$ is a p th power. (As will be shown, the congruence properties of the prime factors of $[(a^p + b^p)/(a + b)]$ when $[(a^p + b^p)/(a + b)]$ is a p th power are similar to the congruence properties of the prime factors of $[(a^p - b^p)/(a - b)]$ when $[(a^p + b^p)/(a + b)]$ is a p th power, but are not the same.)

Let T be a natural number. If $p = 3$, every prime factor of T is of the form $pk + 1$, and T has n such distinct prime factors, then T^p or pT^p has exactly pn representations of the form $(a^p + b^p)/(a + b)$. Proving the first conjecture when p divides $a + b$ would entail proving that if one representation of pT^p of the form $(a^p + b^p)/(a + b)$ exists, then other representations exist and that 2 and p split for some of these representations. There is little evidence that there would exist different representations of pT^p of the form $(a^p + b^p)/(a + b)$ for $p > 3$. Even if there were a representation $((a')^p + (b')^p)/(a' + b')$ with split 2 and p , how to deal with the case where p was a p th power modulo every prime factor of $[(a')^p - (b')^p]/(a' - b')$ not of the form $p^2k + 1$ is unknown.

3 More Congruence Properties of Prime Factors of $[(a^p - b^p)/(a - b)]$ when $[(a^p + b^p)/(a + b)]$ is a p th Power

Let f_1 and f_2 denote relatively prime coefficients of a and b . Propositions involving linear combinations of a and b are;

(17) If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides a , b , $a - b$, or $a + b$, 2 (and not p) is a p th power w.r.t. $(a^p - b^p)/(a - b)$, and one of $a + 2b$, $p(a + 2b)$, $p^2(a + 2b)$, ..., $p^{p-1}(a + 2b)$ is a p th power w.r.t. $(a^p - b^p)/(a - b)$, then (1) $a + 2b$ and $p(2a + b)$, or (2) $2a + b$ and $p(a + 2b)$, or (3) $a + 2b$ and $p^2(2a + b)$, or (4) $2a + b$ and $p^2(a + 2b)$, or (5) $p(a + 2b)$ and $p(2a + b)$, or (6) $p^2(a + 2b)$ and $p^2(2a + b)$ are p th powers w.r.t. $(a^p - b^p)/(a - b)$. If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides a , b , $a - b$, or $a + b$, all the prime factors of $[(a^p - b^p)/(a - b)]$ are not of the form $p^2k + 1$, 2 (and not p) is a p th power w.r.t. $(a^p - b^p)/(a - b)$, and one of $a + 2b$, $p(a + 2b)$, $p^2(a + 2b)$, ..., $p^{p-1}(a + 2b)$ is a p th power w.r.t. $(a^p - b^p)/(a - b)$, then (1) $a + 2b$ and $p(2a + b)$, or (2) $2a + b$ and $p(a + 2b)$, or (3) $a + 2b$ and $p^2(2a + b)$, or (4) $2a + b$ and $p^2(a + 2b)$ are p th powers w.r.t. $(a^p - b^p)/(a - b)$. If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides a , b , $a - b$, or $a + b$, all the prime factors of $[(a^p - b^p)/(a - b)]$ are of the form $p^2k + 1$, and 2 (and not p) is a p th power w.r.t. $(a^p - b^p)/(a - b)$, then (1) $p(a + 2b)$ and

$p(2a+b)$, or (2) $p^2(a+2b)$ and $p^2(2a+b)$ are p th powers w.r.t. $(a^p - b^p)/(a - b)$.

(18) If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides a , b , $a - b$, or $a + b$, and $2p$ (and not 2) is a p th power w.r.t. $(a^p - b^p)/(a - b)$, then (1) $a + 2b$ and $p(2a + b)$, or (2) $2a + b$ and $p(a + 2b)$ are p th powers w.r.t. $(a^p - b^p)/(a - b)$. If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides a , b , $a - b$, or $a + b$, and $p/2$ (and not 2) is a p th power w.r.t. $(a^p - b^p)/(a - b)$, then (1) $p(a + 2b)$ and $p^2(2a + b)$, or (2) $p(2a + b)$ and $p^2(a + 2b)$ are p th powers w.r.t. $(a^p - b^p)/(a - b)$.

(19) If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides a , b , $a - b$, or $a + b$, and p (and not 2) is a p th power w.r.t. $(a^p - b^p)/(a - b)$, then (1) $a + 2b$ and $2(2a + b)$, or (2) $2a + b$ and $2(a + 2b)$ are p th powers w.r.t. $(a^p - b^p)/(a - b)$.

(20) If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ does not divide a , b , $a - b$, or $a + b$, and $2p$ (and not 2) is a p th power w.r.t. $(a^p - b^p)/(a - b)$, then (1) $p(a + 2b)$ and $p^2(2a + b)$, or (2) $p(2a + b)$ and $p^2(a + 2b)$ are p th powers w.r.t. $(a^p - b^p)/(a - b)$.

Let a 6-bit code (for $p = 3$) represent which (if any) of $f_1a + f_2b$, $f_2a + f_1b$, $p(f_1a + f_2b)$, $p(f_2a + f_1b)$, $p^2(f_1a + f_2b)$, $p^2(f_2a + f_1b)$, ..., $p^{p-1}(f_1a + f_2b)$, $p^{p-1}(f_2a + f_1b)$ are p th powers w.r.t. $(a^p - b^p)/(a - b)$. For example, if $p = 3$ and only $p(f_1a + f_2b)$ and $p(f_2a + f_1b)$ are p th powers w.r.t. $(a^p - b^p)/(a - b)$, then the code would be a hexadecimal "c". (When specified, the code may also represent which of $f_1a + f_2b$, $f_2a + f_1b$, $2(f_1a + f_2b)$, $2(f_2a + f_1b)$, $2^2(f_1a + f_2b)$, $2^2(f_2a + f_1b)$, ..., $2^{p-1}(f_1a + f_2b)$, $2^{p-1}(f_2a + f_1b)$ are p th powers w.r.t. $(a^p - b^p)/(a - b)$.)

(21) If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides a , b , $a - b$, or $a + b$, and $2p$ (and not 2) is a p th power w.r.t. $(a^p - b^p)/(a - b)$, then one of $17a + 53b$, $p(17a + 53b)$, $p^2(17a + 53b)$, ..., $p^{p-1}(17a + 53b)$ is a p th power w.r.t. $(a^p - b^p)/(a - b)$ and one of $53a + 17b$, $p(53a + 17b)$, $p^2(53a + 17b)$, ..., $p^{p-1}(53a + 17b)$ is a p th power w.r.t. $(a^p - b^p)/(a - b)$. (f_1, f_2) values, $f_1 < f_2$, where this proposition is true (other than the one listed in Proposition (18)) are (17, 53), (36, 53) (19, 89), (70, 89), (17, 90), (73, 90), (56, 163), (107, 163), (90, 199), (109, 199), (71, 252), (181, 252), (19, 308), (289, 308),

Although the (f_1, f_2) values have been listed in order of increasing f_2 values, they can be ordered into groups of four $((f_1, f_2), (f'_1, f'_2), (f''_1, f''_2), (f'''_1, f'''_2))$ where $f_2 > 2f_1$, $f'_1 = f_2 - f_1$, $f'_2 = f_2$, $f''_1 = f_2 - 2f_1$, $f''_2 = 2f_2 - f_1$, $f'''_1 = f_1 + f_2$, and $f'''_2 = 2f_2 - f_1$. (This is the case for similar results in this section.) In the following table, the codes for the above (f_1, f_2) values are given in a row.

c	21	3	18	12	12	18	3	21	c	12	12	24	24
c	12	3	24	21	21	24	3	12	c	21	21	18	18

There are 2 distinct rows of codes for all a and b that satisfy the above conditions. Such a row of codes will be referred to as a "codeword". For example, for $a = 21762$ and $b = 16271$ (where $(a^p - b^p)/(a - b) = 7 \cdot 1123 \cdot 138967$) and where

the (f_1, f_2) values have been ordered in groups of four as above, the codeword is c, 12, 3, 24, 21, 21, 24, 3, 12, c, 18, 18, 21, 21, 24, 3, 12, c, 18, 18, 21, 21, 24, 3, c, 12, 3, 24, 12, c, 18, 18, c, 12, 3, 24, c, 12, 3, 24, 12, c, 18, 18, 21, 21, 24, 3, 21, 21, 24, 3, 21, 21, 24, 3, For $a = 17783$ and $b = 8910$ (where $(a^p - b^p)/(a - b) = 7 \cdot 3889 \cdot 20353$), the codeword is c, 21, 3, 18, 12, 12, 18, 3, 21, c, 24, 24, 12, 12, 18, 3, 21, c, 24, 24, 12, 12, 18, 3, c, 21, 3, 18, 21, c, 24, 24, c, 21, 3, 18, c, 21, 3, 18, 21, c, 24, 24, 12, 12, 18, 3, 12, 12, 18, 3, 12, 12, 18, 3, Possible code values are 30, c, 3, 18, 6, 21, 12, 9, and 24. A table of (f_1, f_2) , (f'_1, f'_2) , (f''_1, f''_2) , and (f'''_1, f'''_2) values satisfying the above conditions for $f_2 \leq 2000$ is;

(17, 53)	(36, 53)	(19, 89)	(70, 89)
(17, 90)	(73, 90)	(56, 163)	(107, 163)
(90, 199)	(109, 199)	(19, 308)	(289, 308)
(71, 252)	(181, 252)	(110, 433)	(323, 433)
(126, 323)	(197, 323)	(71, 520)	(449, 520)
(179, 540)	(361, 540)	(182, 901)	(719, 901)
(251, 629)	(378, 629)	(127, 1007)	(880, 1007)
(216, 703)	(487, 703)	(271, 1190)	(919, 1190)
(127, 757)	(630, 757)	(503, 1387)	(884, 1387)
(269, 1061)	(792, 1061)	(523, 1853)	(1330, 1853)
(594, 1207)	(613, 1207)	(19, 1820)	(1801, 1820)
(307, 1260)	(953, 1260)	(646, 2213)	(1567, 2213)
(629, 1638)	(1009, 1638)	(380, 2647)	(2267, 2647)
(71, 1890)	(1819, 1890)	(1748, 3709)	(1961, 3709)

The f_1, f'_1, f''_1 , and f'''_1 values are of the form (1) $p^2k_1, p^2k_2 + 1, p^2k_3 + 1$ and $p^2k_4 + 1$, or (2) $p^2k_1, p^2k_2 - 1, p^2k_3 - 1$ and $p^2k_4 - 1$, or (3) $p^2k_1 + 1, p^2k_2, p^2k_3 - 1$ and $p^2k_4 + 2$, or (4) $p^2k_1 + 1, p^2k_2 - 1, p^2k_3 - 2$ and $p^2k_4 + 1$, or (5) $p^2k_1 - 1, p^2k_2, p^2k_3 + 1$ and $p^2k_4 - 2$, or (6) $p^2k_1 - 1, p^2k_2 + 1, p^2k_3 + 2$ and $p^2k_4 - 1$. For a quadratic least-squares fit of the 34 f_2 values (in ascending order) less than or equal to 8000, $p_1 = 5.976$ with a 95% confidence interval of (4.948, 7.004), $p_2 = 33.49$ with a 95% confidence interval of (-3.59, 70.57), $p_3 = 71.69$ with a 95% confidence interval of (-209.8, 353.2), SSE=1.978e+06, R-square=0.9903, and RMSE=252.6 (where $y = p_1x^2 + p_2x + p_3$).

The above (f_1, f_2) values (not grouped) are solutions of $[(a^p + b^p)/(a + b)] = T^p$. The different representations of T^p and pT^p for $p = 3$ account for the groups of four (f_1, f_2) values. If negative f_1 values are allowed, there are groups of six (f_1, f_2) values. The additional (f_1, f_2) values are $(f_1'''' = -f_1, f_2'''' = f_1)$ and $(f_1'''' = -f_1'', f_2'''' = f_1''')$ and correspond to solutions of $[(a^p - b^p)/(a - b)] = T^p$. As expected, there do not appear to be any such codewords when $p = 5, 2p$ (and not 2) is a p th power w.r.t. $(a^p - b^p)/(a - b)$, and $2p$ divides $a, b, a + b$, or $a - b$.

(22) If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides $a, b, a - b$, or $a + b$, $[(a^p - b^p)/(a - b)]$ has exactly two distinct prime factors, $2p$ (and not 2) is a

p th power w.r.t. $(a^p - b^p)/(a - b)$, and one of $a + 3b, p(a + 3b), p^2(a + 3b), \dots, p^{p-1}(a + 3b)$ is a p th power w.r.t. $(a^p - b^p)(a - b)$, then one of $3a + b, p(3a + b), p^2(3a + b), \dots, p^{p-1}(3a + b)$ is a p th power w.r.t. $(a^p - b^p)/(a - b)$. (f_1, f_2) values, $f_1 < f_2$, where this proposition is true (other than the ones listed in Propositions (18) and (21)) are (1, 3), (2, 3), (1, 5), (4, 5), (3, 8), (5, 8), (2, 13), (11, 13), (16, 55), (39, 55), (23, 94), (71, 94), (2, 125), (123, 125), (55, 142), (87, 142), (62, 149), (87, 149), (32, 229), (197, 229), (25, 236), (211, 236), (39, 236), (197, 236), (121, 248), (127, 248), (124, 253), (129, 253),

In the following table, the codewords for (f_1, f_2) values of (1, 3), (2, 3), (1, 5), (4, 5), (3, 8), (5, 8), (2, 13), (11, 13), (16, 55), (39, 55), (23, 94), (71, 94), (2, 125), and (123, 125) are given. There are $2p^2$ distinct codewords for all a and b that satisfy the above conditions.

9	9	21	c	18	3	9	9	30	6	c	21	30	6
24	3	6	6	30	9	c	12	18	18	9	30	18	18
6	6	12	c	24	3	6	6	30	9	c	12	30	9
18	3	9	9	30	6	c	21	24	24	6	30	24	24
30	6	c	21	24	24	6	30	6	30	12	12	6	30
24	24	6	30	6	30	12	12	3	18	30	6	3	18
21	c	24	24	c	21	3	18	12	12	18	3	12	12
9	30	21	21	3	24	30	9	6	6	12	c	6	6
6	30	12	12	3	18	30	6	9	9	21	c	9	9
18	18	9	30	9	30	21	21	3	24	30	9	3	24
c	21	3	18	12	12	18	3	21	c	24	24	21	c
12	12	18	3	21	c	24	24	c	21	3	18	c	21
12	c	18	18	c	12	3	24	21	21	24	3	21	21
30	9	c	12	18	18	9	30	9	30	21	21	9	30
3	18	30	6	9	9	21	c	18	3	9	9	18	3
c	12	3	24	21	21	24	3	12	c	18	18	12	c
3	24	30	9	6	6	12	c	24	3	6	6	24	3
21	21	24	3	12	c	18	18	c	12	3	24	c	12

A continuation of the table for (f_1, f_2) values of (55, 142), (87, 142), (62, 149), (87, 149), (32, 229), (197, 229), (25, 236), (211, 236), (39, 236), (197, 236), (121, 248), (127, 248), (124, 253), and (129, 253) is;

30	6	3	18	c	21	30	6	6	30	c	21	30	6
24	3	6	6	6	6	12	c	3	24	9	30	18	18
30	9	3	24	c	12	30	9	9	30	c	12	30	9
18	3	9	9	9	9	21	c	3	18	6	30	24	24
9	9	18	3	21	c	9	9	9	9	12	12	6	30
3	18	30	6	30	6	c	21	18	3	30	6	3	18
21	c	12	12	24	24	18	3	c	21	18	3	12	12
9	30	18	18	21	21	9	30	30	9	12	c	6	6
6	30	24	24	12	12	6	30	30	6	21	c	9	9
3	24	30	9	30	9	c	12	24	3	30	9	3	24
12	12	21	c	18	3	24	24	12	12	24	24	21	c
c	21	c	21	3	18	3	18	21	c	3	18	c	21
12	c	21	21	18	18	24	3	c	12	24	3	21	21
6	6	24	3	12	c	6	6	6	6	21	21	9	30
24	24	6	30	6	30	12	12	24	24	9	9	18	3
21	21	12	c	24	3	18	18	21	21	18	18	12	c
18	18	9	30	9	30	21	21	18	18	6	6	24	3
c	12	c	12	3	24	3	24	12	c	3	24	c	12

(23) If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ does not divide a , b , $a - b$, or $a + b$, and $2p$ (and not 2) is a p th power w.r.t. $(a^p - b^p)/(a - b)$, then one of $17a + 53b$, $p(17a + 53b)$, $p^2(17a + 53b)$, ..., $p^{p-1}(17a + 53b)$ is a p th power w.r.t. $(a^p - b^p)(a - b)$ and one of $53a + 17b$, $p(53a + 17b)$, $p^2(53a + 17b)$, ..., $p^{p-1}(53a + 17b)$ is a p th power w.r.t. $(a^p - b^p)/(a - b)$. (f_1, f_2) values, $f_1 < f_2$, where this proposition is true (other than the one listed in Proposition (20)) are (17, 53), (36, 53), (19, 89), (70, 89), (17, 90), (73, 90), (56, 163), (107, 163), (90, 199), (109, 199), (71, 252), (181, 252), (19, 308), (289, 308),

In the following table, the codewords for the above (f_1, f_2) values are given. There are 2 distinct codewords for all a and b that satisfy the above conditions.

3	18	30	6	24	24	6	30	18	3	24	24	9	9
3	24	30	9	18	18	9	30	24	3	18	18	6	6

The table of f_1 , f_1' , f_1'' , and f_1''' values satisfying the above conditions is the same as for when $2p$ divides a , b , $a - b$, or $a + b$.

(24) If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides a , b , $a - b$, or $a + b$, and $p/2$ (and not 2) is a p th power w.r.t. $(a^p - b^p)/(a - b)$, then one of $a + 19b$, $p(a + 19b)$, $p^2(a + 19b)$, ..., $p^{p-1}(a + 19b)$ is a p th power w.r.t. $(a^p - b^p)(a - b)$ and one of $19a + b$, $p(19a + b)$, $p^2(19a + b)$, ..., $p^{p-1}(19a + b)$ is a p th power w.r.t. $(a^p - b^p)/(a - b)$. (f_1, f_2) values, $f_1 < f_2$, for which this proposition is true (other than the one listed in Proposition (18)) are (1, 19), (18, 19), (17, 37), (20, 37), (17, 90), (73, 90), (56, 163), (107, 163), (90, 199), (109, 199), (71, 252), (181, 252), (19, 308), (289, 308),

In the following table, the codewords for the above (f_1, f_2) values are given.

There are two distinct codewords for all a and b that satisfy the above conditions.

3	24	30	9	18	18	9	30	24	3	18	18	6	6
3	18	30	6	24	24	6	30	18	3	24	24	9	9

A table of (f_1, f_2) , (f'_1, f'_2) , (f''_1, f''_2) , and (f'''_1, f'''_2) values satisfying the above conditions for $f_2 \leq 1000$ is;

(1, 19)	(18, 19)	(17, 37)	(20, 37)
(17, 90)	(73, 90)	(56, 163)	(107, 163)
(90, 199)	(109, 199)	(19, 308)	(289, 308)
(71, 252)	(181, 252)	(110, 433)	(323, 433)
(126, 323)	(197, 323)	(71, 520)	(449, 520)
(37, 360)	(323, 360)	(286, 683)	(397, 683)
(179, 540)	(361, 540)	(182, 901)	(719, 901)
(251, 629)	(378, 629)	(127, 1007)	(880, 1007)
(216, 703)	(487, 703)	(271, 1190)	(919, 1190)

The f_1, f'_1, f''_1 , and f'''_1 values are of the form (1) $p^2k_1, p^2k_2 + 1, p^2k_3 + 1$ and $p^2k_4 + 1$, or (2) $p^2k_1, p^2k_2 - 1, p^2k_3 - 1$ and $p^2k_4 - 1$, or (3) $p^2k_1 + 1, p^2k_2, p^2k_3 - 1$ and $p^2k_4 + 2$, or (4) $p^2k_1 + 1, p^2k_2 - 1, p^2k_3 - 2$ and $p^2k_4 + 1$, or (5) $p^2k_1 - 1, p^2k_2, p^2k_3 + 1$ and $p^2k_4 - 2$, or (6) $p^2k_1 - 1, p^2k_2 + 1, p^2k_3 + 2$ and $p^2k_4 - 1$. The (f_1, f_2) values (not grouped) are solutions of $[(a^p + b^p)/(a + b)] = T^p$.

(25) If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides $a, b, a - b$, or $a + b$, $[(a^p - b^p)/(a - b)]$ has exactly two distinct prime factors, $p/2$ (and not 2) is a p th power w.r.t. $(a^p - b^p)/(a - b)$, and one of $a + 3b, p(a + 3b), p^2(a + 3b), \dots, p^{p-1}(a + 3b)$ is a p th power w.r.t. $(a^p - b^p)/(a - b)$, then one of $3a + b, p(3a + b), p^2(3a + b), \dots, p^{p-1}(3a + b)$ is a p th power w.r.t. $(a^p - b^p)/(a - b)$. (f_1, f_2) values, $f_1 < f_2$, for which this proposition is true (other than the ones listed in Propositions (18) and (24)) are (1, 3), (2, 3), (1, 5), (4, 5), (3, 8), (5, 8), (2, 13), (11, 13), (16, 55), (39, 55), (23, 94), (71, 94), (62, 149), (87, 149), (25, 236), (211, 236), (39, 236), (197, 236), (124, 253), (129, 253),

In the following table, the codewords for (f_1, f_2) values of (1, 3), (2, 3), (1, 5), (4, 5), (3, 8), (5, 8), (2, 13), (11, 13), (16, 55), (39, 55), (23, 94), and (71, 94) are given. There are $2p^2$ distinct codewords for all a and b that satisfy the above conditions.

3	24	30	9	18	18	9	30	24	3	6	6
12	c	18	18	30	9	c	12	21	21	24	3
6	30	12	12	c	21	3	18	9	9	21	c
12	12	18	3	6	30	12	12	c	21	3	18
18	18	9	30	24	3	6	6	3	24	30	9
21	21	24	3	9	30	21	21	c	12	3	24
9	9	21	c	21	c	24	24	30	6	c	21
21	21	24	3	9	30	21	21	c	12	3	24
6	6	12	c	12	c	18	18	30	9	c	12
c	12	3	24	6	6	12	c	12	c	18	18
18	3	9	9	3	18	30	6	24	24	6	30
30	6	c	21	12	12	18	3	6	30	12	12
9	30	21	21	c	12	3	24	6	6	12	c
c	21	3	18	9	9	21	c	21	c	24	24
30	9	c	12	21	21	24	3	9	30	21	21
21	c	24	24	30	6	c	21	12	12	18	3
24	3	6	6	3	24	30	9	18	18	9	30
3	18	30	6	24	24	6	30	18	3	9	9

(26) If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides a , b , $a - b$, or $a + b$, and p (and not 2) is a p th power w.r.t. $(a^p - b^p)/(a - b)$, then one of $a + 19b$, $2(a + 19b)$, $2^2(a + 19b)$, ..., $2^{p-1}(a + 19b)$ is a p th power w.r.t. $(a^p - b^p)(a - b)$ and one of $19a + b$, $2(19a + b)$, $2^2(19a + b)$, ..., $2^{p-1}(19a + b)$ is a p th power w.r.t. $(a^p - b^p)/(a - b)$. (f_1, f_2) values, $f_1 < f_2$, for which this proposition is true (other than the one listed in Proposition (19)) are (1, 19), (18, 19), (17, 37), (20, 37), (17, 53), (36, 53), (19, 89), (70, 89), (17, 90), (73, 90), (56, 163), (107, 163), (90, 199), (109, 199), (71, 252), (181, 252), (19, 308), (289, 308), (126, 323), (197, 323), (37, 360), (323, 360), (110, 433), (328, 433), (71, 520), (449, 520), (286, 683), (397, 683), ...

In the following table, the codewords for (f_1, f_2) values of (1, 19), (18, 19), (17, 37), (20, 37), (17, 53), (36, 53), (19, 89), (70, 89), (17, 90), (73, 90), (56, 163), (107, 163), (90, 199), and (109, 199) are given. There are two distinct codewords for all a and b that satisfy the above conditions.

3	24	3	24	3	24	3	24	18	18	24	3	24	3
3	18	3	18	3	18	3	18	24	24	18	3	18	3

A table of (f_1, f_2) , (f'_1, f'_2) , (f''_1, f''_2) , and (f'''_1, f'''_2) values satisfying the above conditions for $f_2 \leq 1000$ is;

(1, 19)	(18, 19)	(17, 37)	(20, 37)
(17, 53)	(36, 53)	(19, 89)	(70, 89)
(17, 90)	(73, 90)	(56, 163)	(107, 163)
(90, 199)	(109, 199)	(19, 308)	(289, 308)
(71, 252)	(181, 252)	(110, 433)	(323, 433)
(126, 323)	(197, 323)	(71, 520)	(449, 520)
(37, 360)	(323, 360)	(286, 683)	(397, 683)
(216, 703)	(487, 703)	(271, 1190)	(919, 1190)
(127, 757)	(630, 757)	(503, 1387)	(884, 1387)
(270, 971)	(701, 971)	(431, 1672)	(1241, 1672)
(359, 990)	(631, 990)	(272, 1621)	(1349, 1621)

The f_1 , f_1' , f_1'' , and f_1''' values are of the form (1) $p^2k_1, p^2k_2 + 1, p^2k_3 + 1$ and $p^2k_4 + 1$, or (2) $p^2k_1, p^2k_2 - 1, p^2k_3 - 1$ and $p^2k_4 - 1$, or (3) $p^2k_1 + 1, p^2k_2, p^2k_3 - 1$ and $p^2k_4 + 2$, or (4) $p^2k_1 + 1, p^2k_2 - 1, p^2k_3 - 2$ and $p^2k_4 + 1$, or (5) $p^2k_1 - 1, p^2k_2, p^2k_3 + 1$ and $p^2k_4 - 2$, or (6) $p^2k_1 - 1, p^2k_2 + 1, p^2k_3 + 2$ and $p^2k_4 - 1$. The (f_1, f_2) values (not grouped) are solutions of $[(a^p + b^p)/(a + b)] = T^p$.

(27) If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides $a, b, a - b$, or $a + b, p$ (and not 2) is a p th power w.r.t. $(a^p - b^p)/(a - b)$, $[(a^p - b^p)/(a - b)]$ has exactly two distinct prime factors, and one of $a + 3b, 2(a + 3b), 2^2(a + 3b), \dots, 2^{p-1}(a + 3b)$ is a p th power w.r.t. $(a^p - b^p)(a - b)$, then one of $3a + b, 2(3a + b), 2^2(3a + b), \dots, 2^{p-1}(3a + b)$ is a p th power w.r.t. $(a^p - b^p)/(a - b)$. (f_1, f_2) values, $f_1 < f_2$, for which this proposition is true (other than the ones listed in Propositions (19) and (26)) are (1, 3), (2, 3), (1, 5), (4, 5), (3, 8), (5, 8), (2, 13), (11, 13), (16, 55), (39, 55), (23, 94), (71, 94), (2, 125), (123, 125), (55, 142), (87, 142), (62, 149), (87, 149), ...

In the following table, the codewords for (f_1, f_2) values of (1, 3), (2, 3), (1, 5), (4, 5), (3, 8), (5, 8), (2, 13), (11, 13), (16, 55), (39, 55), (23, 94), and (71, 94) are given. There are $2p^2$ distinct codewords for all a and b that satisfy the above condition.

21	c	12	12	30	6	30	6	12	12	21	c
30	9	30	9	21	21	12	c	9	30	6	6
12	c	21	21	30	9	30	9	21	21	12	c
9	30	6	6	c	12	c	12	6	6	9	30
6	30	9	9	c	21	c	21	9	9	6	30
30	6	30	6	12	12	21	c	6	30	9	9
3	18	3	18	24	24	18	3	18	3	24	24
24	24	18	3	18	3	24	24	3	18	3	18
c	12	c	12	6	6	9	30	12	c	21	21
3	24	3	24	18	18	24	3	24	3	18	18
18	3	24	24	3	18	3	18	24	24	18	3
9	9	6	30	21	c	12	12	30	6	30	6
12	12	21	c	6	30	9	9	c	21	c	21
18	18	24	3	24	3	18	18	3	24	3	24
24	3	18	18	3	24	3	24	18	18	24	3
6	6	9	30	12	c	21	21	30	9	30	9
c	21	c	21	9	9	6	30	21	c	12	12
21	21	12	c	9	30	6	6	c	12	c	12

(28) If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides a , b , $a - b$, or $a + b$, and 2 (and not p) is a p th power w.r.t. $(a^p - b^p)/(a - b)$, then one of $a + 19b$, $p(a + 19b)$, $p^2(a + 19b)$, ..., $p^{p-1}(a + 19b)$ is a p th power w.r.t. $(a^p - b^p)(a - b)$ and one of $19a + b$, $p(19a + b)$, $p^2(19a + b)$, ..., $p^{p-1}(19a + b)$ is a p th power w.r.t. $(a^p - b^p)/(a - b)$. (f_1, f_2) values, $f_1 < f_2$, for which this proposition is true are (1, 19), (17, 37), (17, 53), (19, 89), (251, 629), (127, 1007), (127, 757), (503, 1387), (269, 1061), (523, 1853), (233, 1637), (1171, 3041), (703, 1873), (467, 3043),

In the following table, the codewords for the above (f_1, f_2) values are given. There are two distinct codewords for all a and b that satisfy the above conditions.

c	3	c	3	c	3	c	3	c	3	c	3	c	3
30	c	30	c	30	c	30	c	30	c	30	c	30	c

(29) If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides a , b , $a - b$, or $a + b$, 2 (and not p) is a p th power w.r.t. $(a^p - b^p)/(a - b)$, and one of $18a + 19b$, $p(18a + 19b)$, $p^2(18a + 19b)$, ..., $p^{p-1}(18a + 19b)$ is a p th power w.r.t. $(a^p - b^p)(a - b)$, then one of $19a + 18b$, $p(19a + 18b)$, $p^2(19a + 18b)$, ..., $p^{p-1}(19a + 18b)$ is a p th power w.r.t. $(a^p - b^p)/(a - b)$. (f_1, f_2) values, $f_1 < f_2$, for which this proposition is true (including (f_1, f_2) values listed in Proposition (28)) are (1, 19), (18, 19), (17, 37), (20, 37), (17, 53), (36, 53), (19, 89), (70, 89), (251, 629), (378, 629), (127, 1007), (880, 1007), (127, 757), (630, 757), (503, 1387), (884, 1387), (269, 1061), (792, 1061), (523, 1853), (1330, 1853), (233, 1637), (1404, 1637), (1171, 3041), (1870, 3041), (703, 1873), (1170, 1873), (467, 3043), (2576, 3043), Note that the (f_1, f_2) values have been ordered in the groups of four.

In the following table, the codewords for (f_1, f_2) values of (1, 19), (18, 19), (17,

37), (20, 37), (17, 53), (36, 53), (19, 89), (70, 89), (251, 629), (378, 629), (127, 1007), (880, 1007), (127, 757), (630, 757), (503, 1387), (884, 1387), (269, 1061), (792, 1061), (523, 1853), and (1330, 1853) are given. There are $2p$ distinct code-words for all a and b that satisfy the above conditions.

c	21	3	18	c	21	3	18	c	21	3	18	c	21	3	18	c	21	3	18
30	9	c	12	30	9	c	12	30	9	c	12	30	9	c	12	30	9	c	12
c	c	3	3	c	c	3	3	c	c	3	3	c	c	3	3	c	c	3	3
c	12	3	24	c	12	3	24	c	12	3	24	c	12	3	24	c	12	3	24
30	30	c	c	30	30	c	c	30	30	c	c	30	30	c	c	30	30	c	c
30	6	c	21	30	6	c	21	30	6	c	21	30	6	c	21	30	6	c	21

Converting the hexadecimal codes in the second column into binary gives the following $2p$ by $2p$ matrix.

1	0	0	0	0	1
0	0	1	0	0	1
0	0	1	1	0	0
0	1	0	0	1	0
1	1	0	0	0	0
0	0	0	1	1	0

The real-valued eigenvalues of this matrix are 0 and 2 and the respective eigenvectors are $(-1, 1, -1, 1, -1, 1)$ and $(1, 1, 1, 1, 1, 1)$. Converting the hexadecimal codes in the fourth column into binary gives the following $2p$ by $2p$ matrix;

0	1	1	0	0	0
0	1	0	0	1	0
0	0	0	0	1	1
1	0	0	1	0	0
0	0	1	1	0	0
1	0	0	0	0	1

The real-valued eigenvalues of this matrix are 0, 2, -1, and 1 and the respective eigenvectors are $(-1, 1, -1, 1, -1, 1)$, $(1, 1, 1, 1, 1, 1)$, $(-2, 1, 1, 1, -2, 1)$, and $(0, -1, 1, -1, 0, 1)$. (See the preface of Diamond and Shurman's [3] book for a discussion of the relationship between the modularity theorem and a re-interpretation of the quadratic reciprocity theorem as a system of eigenvalues on a finite-dimensional complex vector space. Also, see Shurman [4]. The normalized solution counts are given by the Jacobi symbol. Here, 0's and 1's give the solution counts.)

A table of (f_1, f_2) , (f'_1, f'_2) , (f''_1, f''_2) , and (f'''_1, f'''_2) values satisfying the above conditions for $f_2 \leq 4000$ is;

(1, 19)	(18, 19)	(17, 37)	(20, 37)
(17, 53)	(36, 53)	(19, 89)	(70, 89)
(251, 629)	(378, 629)	(127, 1007)	(880, 1007)
(127, 757)	(630, 757)	(503, 1387)	(884, 1387)
(269, 1061)	(792, 1061)	(523, 1853)	(1330, 1853)
(233, 1637)	(1404, 1637)	(1171, 3041)	(1870, 3041)
(703, 1873)	(1170, 1873)	(467, 3043)	(2576, 3043)
(1007, 2393)	(1386, 2393)	(379, 3779)	(3400, 3779)
(739, 2719)	(1980, 2719)	(1241, 4699)	(3458, 4699)

The $f_1, f_1', f_1'',$ and f_1''' values are of the form (1) $p^2k_1, p^2k_2 + 1, p^2k_3 + 1$ and $p^2k_4 + 1$, or (2) $p^2k_1, p^2k_2 - 1, p^2k_3 - 1$ and $p^2k_4 - 1$, or (3) $p^2k_1 + 1, p^2k_2, p^2k_3 - 1$ and $p^2k_4 + 2$, or (4) $p^2k_1 + 1, p^2k_2 - 1, p^2k_3 - 2$ and $p^2k_4 + 1$, or (5) $p^2k_1 - 1, p^2k_2, p^2k_3 + 1$ and $p^2k_4 - 2$, or (6) $p^2k_1 - 1, p^2k_2 + 1, p^2k_3 + 2$ and $p^2k_4 - 1$. The (f_1, f_2) values (not grouped) are solutions of $[(a^p + b^p)/(a + b)] = T^p$. The (f_1, f_2) and (f_1'', f_2'') values satisfy the conditions of Proposition (28) and the (f_1', f_2') and (f_1''', f_2''') values satisfy the conditions of Proposition (29).

(30) If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides $a, b, a - b$, or $a + b$, and 2 (and not p) is a p th power w.r.t. $(a^p - b^p)/(a - b)$, then one of $107a + 163b, p(107a + 163b), p^2(107a + 163b), \dots, p^{p-1}(107a + 163b)$ is a p th power w.r.t. $(a^p - b^p)(a - b)$ and one of $163a + 107b, p(163a + 107b), p^2(163a + 107b), \dots, p^{p-1}(163a + 107b)$ is a p th power w.r.t. $(a^p - b^p)/(a - b)$. (f_1, f_2) values, $f_1 < f_2$, for which this proposition is true (excluding the (f_1, f_2) values listed in Proposition (28)) are (107, 163), (323, 433), (397, 683), (719, 901), (487, 703), (701, 971), (1349, 1621), (613, 1207), (1297, 1693), (1961, 3709), (2033, 3203), (2701, 3331),

In the following table, the codewords for the above (f_1, f_2) values are given. There are two distinct codewords for all a and b that satisfy the above conditions.

3	3	3	3	c	c	3	c	c	3	c	c
c	c	c	c	30	30	c	30	30	c	30	30

(31) If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides $a, b, a - b$, or $a + b$, 2 (and not p) is a p th power w.r.t. $(a^p - b^p)/(a - b)$, and one of $17a + 90b, p(17a + 90b), p^2(17a + 90b), \dots, p^{p-1}(17a + 90b)$ is a p th power w.r.t. $(a^p - b^p)(a - b)$, then one of $90a + 17b, p(90a + 17b), p^2(90a + 17b), \dots, p^{p-1}(90a + 17b)$ is a p th power w.r.t. $(a^p - b^p)/(a - b)$. (f_1, f_2) values, $f_1 < f_2$, for which this proposition is true (excluding the (f_1, f_2) values listed in Proposition (29) and including the (f_1, f_2) values listed in Proposition (30)) are (17, 90), (73, 90), (56, 163), (107, 163), (71, 252), (181, 252), (110, 433), (323, 433), (37, 360), (323, 360), (286, 683), (397, 683), (179, 540), (361, 540), (182, 901), (719, 901), (216, 703), (487, 703), (271, 1190), (919, 1190), Note that the (f_1, f_2) values have been ordered in the groups of four.

In the following table, the codewords for (f_1, f_2) values of (17, 90), (73, 90),

(56, 163), (107, 163), (71, 252), (181, 252), (110, 433), (323, 433), (37, 360), (323, 360), (286, 683), (397, 683), (179, 540), (361, 540), (182, 901), (719, 901), (216, 703), (487, 703), (271, 1190), and (1919, 1190) are given. There are $2p$ distinct codewords for all a and b that satisfy the above conditions.

12	12	18	3	12	12	18	3	12	12	18	3	12	12	18	3	21	c	24	24
6	6	12	c	6	6	12	c	6	6	12	c	6	6	12	c	9	30	21	21
c	c	3	3	c	c	3	3	c	c	3	3	c	c	3	3	c	c	3	3
21	21	24	3	21	21	24	3	21	21	24	3	21	21	24	3	12	c	18	18
30	30	c	c	30	30	c	c	30	30	c	c	30	30	c	c	30	30	c	c
9	9	21	c	9	9	21	c	9	9	21	c	9	9	21	c	6	30	12	c

Converting the hexadecimal codes in the first column into binary gives the following $2p$ by $2p$ matrix.

0	1	0	0	1	0
0	0	0	1	1	0
0	0	1	1	0	0
1	0	0	0	0	1
1	1	0	0	0	0
0	0	1	0	0	1

The real-valued eigenvalues of this matrix are 0, 2, -1, and 1.4656 and the respective eigenvectors are (-1, 1, -1, 1, -1, 1), (1, 1, 1, 1, 1, 1), (0, -1, 0, 0, 1, 0), and (-0.6823, -0.3177, 0.4656, 0.2168, -0.6823, 1). Converting the hexadecimal codes in the nineteenth column into binary gives the following $2p$ by $2p$ matrix;

1	0	0	1	0	0
1	0	0	0	0	1
0	0	0	0	1	1
0	1	1	0	0	0
0	0	1	1	0	0
0	1	0	0	1	0

The real-valued eigenvalues of this matrix are 0, 2, -1, and 1 and the respective eigenvectors are (-1, 1, -1, 1, -1, 1), (1, 1, 1, 1, 1, 1), (-1, -1, -1, 2, -1, 2), and (-1, -1, 1, 0, 1, 0).

A table of (f_1, f_2) , (f'_1, f'_2) , (f''_1, f''_2) , and (f'''_1, f'''_2) values satisfying the above conditions for $f_2 \leq 4000$ is;

(17, 90)	(73, 90)	(56, 163)	(107, 163)
(71, 252)	(181, 252)	(110, 433)	(323, 433)
(37, 360)	(323, 360)	(286, 683)	(397, 683)
(179, 540)	(361, 540)	(182, 901)	(719, 901)
(216, 703)	(487, 703)	(271, 1190)	(919, 1190)
(270, 971)	(701, 971)	(431, 1672)	(1241, 1672)
(359, 990)	(631, 990)	(272, 1621)	(1349, 1621)
(594, 1207)	(613, 1207)	(19, 1820)	(1801, 1820)
(396, 1693)	(1297, 1693)	(901, 2990)	(2089, 2990)
(71, 1890)	(1819, 1890)	(1748, 3709)	(1961, 3709)
(1170, 3203)	(2033, 3203)	(863, 5236)	(4373, 5236)
(630, 3331)	(2701, 3331)	(2071, 6032)	(3961, 6032)

The $f_1, f_1', f_1'',$ and f_1''' values are of the form (1) $p^2k_1, p^2k_2 + 1, p^2k_3 + 1$ and $p^2k_4 + 1$, or (2) $p^2k_1, p^2k_2 - 1, p^2k_3 - 1$ and $p^2k_4 - 1$, or (3) $p^2k_1 + 1, p^2k_2, p^2k_3 - 1$ and $p^2k_4 + 2$, or (4) $p^2k_1 + 1, p^2k_2 - 1, p^2k_3 - 2$ and $p^2k_4 + 1$, or (5) $p^2k_1 - 1, p^2k_2, p^2k_3 + 1$ and $p^2k_4 - 2$, or (6) $p^2k_1 - 1, p^2k_2 + 1, p^2k_3 + 2$ and $p^2k_4 - 1$. The (f_1, f_2) values (not grouped) are solutions of $[(a^p + b^p)/(a + b)] = T^p$. The (f_1, f_2) and (f_1'', f_2'') values satisfy the conditions of Proposition (31). Exactly one of each pair of (f_1', f_2') and (f_1''', f_2''') values satisfies the conditions of Proposition (30).

The (f_1, f_2) values (not grouped) in Proposition (21) (where $2p$ is a p th power w.r.t. $(a^p - b^p)/(a - b)$), Proposition (24) (where $p/2$ is a p th power w.r.t. $(a^p - b^p)/(a - b)$), Proposition (26) (where p is a p th power w.r.t. $(a^p - b^p)/(a - b)$), and Propositions (29) and (31) (where 2 is a p th power w.r.t. $(a^p - b^p)/(a - b)$) appear to account for all solutions of $[(a^p + b^p)/(a + b)] = T^p$ (and $[(a^p - b^p)/(a - b)] = T^p$ if negative f_1 values are allowed). It appears that there are solutions of $[(a^p + b^p)/(a + b)] = T^p$ only if such codewords exist.

(32) If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides $a, b, a - b$, or $a + b$, and 2 and p are p th powers w.r.t. $(a^p - b^p)/(a - b)$, then $a + 19b$ and $19a + b$ are p th powers w.r.t. $(a^p - b^p)/(a - b)$. (f_1, f_2) values, $f_1 < f_2$, for which this proposition is true are (1, 19), (17, 37), (17, 53), (19, 89), (107, 163), (109, 199), (197, 323), (323, 433),

(33) If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides $a, b, a - b$, or $a + b$, 2 and p are p th powers w.r.t. $(a^p - b^p)/(a - b)$, and $a + 2b$ is a p th power w.r.t. $(a^p - b^p)/(a - b)$, then $2a + b$ is a p th power w.r.t. $(a^p - b^p)/(a - b)$. (f_1, f_2) values, $f_1 < f_2$, for which this proposition is true (excluding the (f_1, f_2) values listed in Proposition (32)) are (1, 2), (18, 19), (20, 37), (36, 53), (70, 89), (17, 90), (73, 90), (56, 163), (90, 199), (71, 252), (181, 252), (19, 308), (289, 308), (126, 323), (37, 360), (323, 360), (110, 433), These (f_1, f_2) values combined with the ones in Proposition (32) appear to consist of all the solutions of $[(a^p + b^p)/(a + b)] = T^p$, including the ones where $2p$ does not divide $a, b, a - b$, or $a + b$.

4 Mordell's Conjecture and Faltings' Theorem

Mordell [5] conjectured that a curve of genus greater than 1 over a number field has only finitely many rational points and Faltings [6] proved this. A consequence of Faltings' theorem is a weak form of Fermat's Last Theorem, that is, for any $n > 4$ there are at most finitely many primitive integer solutions of $a^n + b^n = c^n$ since for such n the curve $x^n + y^n = 1$ has genus greater than 1.

There are 12816 solutions of $[(a^p + b^p)/(a + b)] = T^p$ for $p = 3$ when a and b are less than 5 million (excluding $(a, b) = (1, 2)$). Of these, there are 1167 solutions that satisfy the conditions of Proposition (32) and 1167 solutions that satisfy the conditions of Proposition (33) when $(a^p - b^p)/(a - b)$ has exactly one distinct prime factor. When $(a^p - b^p)/(a - b)$ has exactly two distinct prime factors, there are 339 solutions that satisfy the conditions of Proposition (32), but only 186 solutions that satisfy the conditions of Proposition (33). When $(a^p - b^p)/(a - b)$ has exactly three distinct prime factors, there are 21 solutions that satisfy the conditions of Proposition (32), but only 2 solutions that satisfy the conditions of Proposition (33).

The number of solutions of $[(a^p + b^p)/(a + b)] = T^p$, $p = 3$, where a and b are less than or equal to 10000, 20000, 30000, ..., 200000 are 200, 320, 422, 508, 594, 678, 744, 816, 874, 948, 1006, 1066, 1116, 1174, 1232, 1286, 1346, 1388, 1456, and 1500 respectively. For a quadratic least-squares fit of these counts, SSE=4269, R-square=0.9985, and RMSE=15.85. Let n denote the number of solutions of $[(a^p + b^p)/(a + b)] = T^p$, $p = 3$, less than or equal to a specified upper bound. In the following, the number of (f_1, f_2) and (a, b) values such that $f_1a + f_2b$ and $f_2a + f_1b$ are p th powers w.r.t. $(a^p - b^p)/(a - b)$ are counted. The (f_1, f_2) values are just the (a, b) values (in accordance with Propositions (32) and (33)), so up to n^2 combinations of (f_1, f_2) and (a, b) values may be considered. If $n = 10000$, $2p$ divides a , b , $a - b$, or $a + b$, 2 and p are p th powers w.r.t. $(a^p - b^p)/(a - b)$, and $(a^p - b^p)/(a - b)$ has exactly one distinct prime factor, then the solution count for each (f_1, f_2) value is 36. The solution counts for n equal to 10000, 20000, 30000, ..., 200000 are 36, 51, 58, 67, 77, 85, 92, 103, 107, 116, 120, 127, 131, 140, 144, 149, 154, 159, 171, and 176 respectively. For a quadratic least-squares fit of these counts, SSE=115.7, R-square=0.9964, and RMSE=2.609. For $n = 10000$, a measure of the "density" of these solutions is $(\sqrt{36 \cdot 200})/200$ or about 0.4243. The densities for $n = 10000, 20000, 30000, \dots, 200000$ are 0.4243, 0.3992, 0.3707, 0.3632, 0.3600, 0.3541, 0.3516, 0.3553, 0.3499, 0.3498, 0.3454, 0.3452, 0.3426, 0.3453, 0.3419, 0.3404, 0.3383, 0.3385, 0.3427, and 0.3425 respectively. The densities appear to decrease at about the same rate as $1/\log(x)$, $x = 2, 3, 4, \dots, 20$.

If $n = 10000$, $2p$ divides a , b , $a - b$, or $a + b$, 2 and p are p th powers w.r.t. $(a^p - b^p)/(a - b)$, and $(a^p - b^p)/(a - b)$ has exactly two distinct prime factors, then the solution count for each (f_1, f_2) value is 2. If $n = 20000$, $2p$ divides a , b , $a - b$, or $a + b$, 2 and p are p th powers w.r.t. $(a^p - b^p)/(a - b)$,

and $(a^p - b^p)/(a - b)$ has exactly two distinct prime factors, then the solution count for each (f_1, f_2) value is 6 or 2. The solution counts for n equal to 10000, 20000, 30000, ..., 200000 are (2, 2), (6, 2), (8, 4), (11, 5), (13, 7), (17, 10), (19, 10), (22, 11), (24, 13), (25, 13), (27, 13), (27, 13), (30, 14), (33, 15), (34, 16), (35, 17), (36, 17), (36, 17), (39, 19), and (40, 20) respectively. For a quadratic least-squares fit of the larger counts, SSE=11.49, R-square=0.9955, and RMSE=0.8221. For a quadratic least-squares fit of the smaller counts, SSE=14.65, R-square=0.9742, and RMSE=0.9282. Let x denote the number of times the solution count takes the larger value and y the number of times the solution count takes the smaller value. For $n = 20000$, a measure of the density of the solutions is $(\sqrt{(6x + 2y)})/320$ or about 0.1019. The densities for $n = 10000, 20000, 30000, \dots, 200000$ are 0.1, 0.1019, 0.1118, 0.1169, 0.1224, 0.1340, 0.1314, 0.1330, 0.1371, 0.1327, 0.1307, 0.1269, 0.1298, 0.1319, 0.1319, 0.1321, 0.1300, 0.1280, 0.1312, and 0.1315 respectively. The densities appear to slowly increase.

When $(a^p - b^p)/(a - b)$ has only one distinct prime factor, the solutions of $[(a^p + b^p)/(a + b)] = T^p$ appear to be “closed”. That is, no matter what upper bound of the (a, b) values that is chosen, there are no solutions of $[(a^p + b^p)/(a + b)] = T^p$ other than the (f_1, f_2) values corresponding to (or “generated by”) the solutions that satisfy the conditions of Propositions (32) and (33). This is not the case when $(a^p - b^p)/(a - b)$ has more than one distinct prime factor. For example, for the 410 smallest solutions of $[(a^p + b^p)/(a + b)] = T^p$, $a < b$, the largest solution is (7812, 28981). The solutions (6697, 10640), (3943, 10640), (4861, 5779), and (918, 5779) are not generated by the solutions that satisfy Propositions (32) and (33) when $(a^p - b^p)/(a - b)$ has exactly two distinct prime factors. Of course, there appear to be infinitely many solutions of $[(a^p + b^p)/(a + b)] = T^p$ when $p = 3$.

(a, b) values that satisfy Proposition (32) or (33) generate themselves. In this case, $a^2 + b^2$ and $2ab$ (or ab) are p th powers w.r.t. $(a^p - b^p)/(a - b)$. Note that this is not necessarily inconsistent with Proposition (12). A less general version of Proposition (12) is;

If $[(a^p + b^p)/(a + b)]$ is a p th power and p is a p th power w.r.t. $(a^p - b^p)/(a - b)$, then a is a p th power w.r.t. $(a^p - b^p)/(a - b)$ if $2p$ divides a , or b is a p th power w.r.t. $(a^p - b^p)/(a - b)$ if $2p$ divides b , or $a - b$ and $a + b$ are p th powers w.r.t. $(a^p - b^p)/(a - b)$ if $2p$ divides $a - b$ or $a + b$.

When $p = 3$, $(a^p - b^p)/(a - b)$ equals $a^2 + ab + b^2$, so the conditions that $a^2 + b^2$ and ab are p th powers w.r.t. $(a^p - b^p)/(a - b)$ are less stringent and reduce to the condition that ab is a p th power w.r.t. $(a^p - b^p)/(a - b)$.

If $p = 5$, $2p$ divides $a, b, a - b$, or $a + b$, and 2 and p are p th powers w.r.t. $(a^p - b^p)/(a - b)$, then p^2 divides $a, b, a - b$, or $a + b$ and $a, b, a - b$, and $a + b$ are p th powers w.r.t. $(a^p - b^p)/(a - b)$. When $p = 5$, there is no “reciprocity” rela-

tionship, that is, $f_1a + f_2b$ is a p th power w.r.t. $(a^p - b^p)/(a - b)$ does not imply that $f_2a + f_1b$ is a p th power w.r.t. $(a^p - b^p)/(a - b)$. Whether $(a^p - b^p)/(a - b)$ has exactly one distinct prime factor is still of significance (by virtue of their being more plentiful than all the solutions having more than one distinct prime factor combined). When $p = 5$ and a and b are less than or equal to 1000, there are 2037 (a, b) values such that $2p$ divides a , b , $a - b$, or $a + b$, 2 and p are p th powers w.r.t. $(a^p - b^p)/(a - b)$, and $(a^p - b^p)/(a - b)$ has exactly one distinct prime factor. The (f_1, f_2) values are then assigned these values and the numbers of times $f_1a + f_2b$ and $f_2a + f_1b$ are p th powers w.r.t. $(a^p - b^p)/(a - b)$ are counted. For each (f_1, f_2) value, the number of solutions ranges from 54 to 122. See Figure 1 for the histogram of the solution counts. Using the estimated mean and standard deviation (within 95% confidence intervals) gives the normal probability plot in Figure 2. The linearity of the plot indicates that the data came from a normal probability distribution. The number of times an (a, b) value generates itself is 1241. In this case, whether $a^2 + b^2$ is a p th power w.r.t. $(a^p - b^p)/(a - b)$ is non-trivial. The density (computed similarly to the way it was for $p = 3$) is 0.2022.

When $p = 5$ and a and b are less than or equal to 1000, there are 131 (a, b) values such that $2p$ divides a , b , $a - b$, or $a + b$, 2 and p are p th powers w.r.t. $(a^p - b^p)/(a - b)$, and $(a^p - b^p)/(a - b)$ has exactly two distinct prime factors. The (f_1, f_2) values are then assigned these values. For 109 (f_1, f_2) values, there are no instances where $f_1a + f_2b$ and $f_2a + f_1b$ are p th powers w.r.t. $(a^p - b^p)/(a - b)$. For the remaining (f_1, f_2) values, the number of solutions is 1 or 2. An (a, b) value generates itself once. The density is 0.0366 (approximately equal to the square of the density when $(a^p - b^p)/(a - b)$ had only one distinct prime factor).

When $p = 5$ and a and b are less than or equal to 1000, there is 1 (a, b) values such that $2p$ divides a , b , $a - b$, or $a + b$, 2 and p are p th powers w.r.t. $(a^p - b^p)/(a - b)$, and $(a^p - b^p)/(a - b)$ has exactly three distinct prime factors. Another approach is to set the (f_1, f_2) values to this (a, b) value and to the (a, b) values where $(a^p - b^p)/(a - b)$ had exactly two distinct primes factors. The (a, b) values are then set to only the (a, b) values where $(a^p - b^p)/(a - b)$ had exactly one distinct prime factor. The numbers of times $f_1a + f_2b$ and $f_2a + f_1b$ are p th powers w.r.t. $(a^p - b^p)/(a - b)$ are then counted. For each (f_1, f_2) value, the number of solutions ranges from 59 to 105. See Figure 3 for the histogram of the solution counts. Using the estimated mean and standard deviation (within 95% confidence intervals) gives the normal probability plot in Figure 4. The linearity of the plot indicates that the data came from a normal probability distribution. This normal distribution appears to be independent of the above normal distribution.

If $p = 7$, $2p$ divides a , b , $a - b$, or $a + b$, and 2 and p are p th powers w.r.t. $(a^p - b^p)/(a - b)$, then p^2 divides a , b , $a - b$, or $a + b$ and a , b , $a - b$, and $a + b$ are p th powers w.r.t. $(a^p - b^p)/(a - b)$. When $p = 7$ and a and b are less than or equal to 700, there are 525 (a, b) values such that $2p$ divides a , b , $a - b$, or

$a + b$, 2 and p are p th powers w.r.t. $(a^p - b^p)/(a - b)$, and $(a^p - b^p)/(a - b)$ has exactly one distinct prime factor. The (f_1, f_2) values are then assigned these values and the numbers of times $f_1a + f_2b$ and $f_2a + f_1b$ are p th powers w.r.t. $(a^p - b^p)/(a - b)$ are counted. For each (f_1, f_2) value, the number of solutions ranges from 4 to 28. See Figure 5 for the histogram of the solution counts. Using the estimated mean and standard deviation (within 95% confidence intervals) gives the normal probability plot in Figure 6. The linearity of the plot indicates that the data came from a normal probability distribution. The number of times an (a, b) value generates itself is 311. The density is 0.1518.

When $p = 7$ and a and b are less than or equal to 700, there are 16 (a, b) values such that $2p$ divides a , b , $a - b$, or $a + b$, 2 and p are p th powers w.r.t. $(a^p - b^p)/(a - b)$, and $(a^p - b^p)/(a - b)$ has exactly two distinct prime factors. The (f_1, f_2) values are then assigned these values and the numbers of times $f_1a + f_2b$ and $f_2a + f_1b$ are p th powers w.r.t. $(a^p - b^p)/(a - b)$ are counted. For 15 of the (f_1, f_2) values, the number of solutions is 0. For the remaining (f_1, f_2) value, the number of solutions is 1. This (a, b) value doesn't generate itself. The density is 0.0625.

For $p = 3$, there appear to be solutions of $[(a^p + b^p)/(a + b)] = T^p$ if and only if there are generators. For $p > 3$, there appear to be infinitely many generators for every p value. For each p value, the generators have characteristics similar to those for $p = 3$, the main difference being that there is no "reciprocity" relationship for $p > 3$.

5 Congruence Properties of Prime $[(a^p - b^p)/(a - b)]$ when $[(a^p + b^p)]$ is a p th Power

In this section, more empirical evidence in support of Propositions (8), (12), and (13) is given. The following propositions are based on data collected for $p = 3, 5, 7$, and 11;

(34) If $p > 3$, p^2 divides a , b , $a - b$, or $a + b$, $[(a^p + b^p)/(a + b)]$ and $[(a^p - b^p)/(a - b)]$ are primes of the form $p^2k + 1$, and 2 is a p th power modulo $[(a^p + b^p)/(a + b)]$ or $[(a^p - b^p)/(a - b)]$, then $[(a^p - b^p)/(a - b)]$ is a p th power modulo $[(a^p + b^p)/(a + b)]$ and $[(a^p + b^p)/(a + b)]$ is a p th power modulo $[(a^p - b^p)/(a - b)]$. An analogous result holds for $p = 3$ if p^2 divides a or b or p^3 divides $a - b$ or $a + b$.

(35) If $[(a^p - b^p)/(a - b)]$ is prime, $q^{p-1} \equiv 1 \pmod{p^2}$, and q divides a , b , $a + b$, or $a - b$, then q is a p th power modulo $[(a^p - b^p)/(a - b)]$.

(36) If $p > 3$, $[(a^p - b^p)/(a - b)]$ is prime, and p^2 divides a , b , $a + b$, or $a - b$, then p is a p th power modulo $[(a^p - b^p)/(a - b)]$. If $p = 3$, $[(a^p - b^p)/(a - b)]$ is prime, and p^2 divides a , b , or $a + b$ or p^3 divides $a - b$, then p is a p th power

modulo $[(a^p - b^p)/(a - b)]$.

(37) If $[(a^p - b^p)/(a - b)]$ is prime, p does not divide q , p divides a and q divides a , or p divides b and q divides b , or p divides $a + b$ and q divides $a + b$ or $a - b$, then q is a p th power modulo $[(a^p - b^p)/(a - b)]$. If $p > 3$, $[(a^p - b^p)/(a - b)]$ is prime, p does not divide q , p divides $a - b$, and q divides $a + b$ or $a - b$, then q is a p th power modulo $[(a^p - b^p)/(a - b)]$. If $p = 3$, $[(a^p - b^p)/(a - b)]$ is prime, p does not divide q , p^2 divides $a - b$, and q divides $a + b$ or $a - b$, then q is a p th power modulo $[(a^p - b^p)/(a - b)]$.

(38) If $p > 3$, $[(a^p - b^p)/(a - b)]$ is a prime of the form $p^2k + 1$, and p^2 divides a , b , $a + b$, or $a - b$, then a , b , $a + b$, $a - b$, and p are p th powers modulo $[(a^p - b^p)/(a - b)]$. If $p = 3$, $[(a^p - b^p)/(a - b)]$ is a prime of the form $p^2k + 1$, and p^2 divides a , b , or $a + b$ or p^3 divides $a - b$, then a , b , $a + b$, $a - b$, and p are p th powers modulo $[(a^p - b^p)/(a - b)]$.

Propositions (35), (36), (37) and Propositions (5) and (6) lead to the following proposition;

(39) If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides a , b , $a - b$, or $a + b$, and $[(a^p - b^p)/(a - b)]$ is prime, then every factor of a , b , $a - b$, and $a + b$ is a p th power modulo $[(a^p - b^p)/(a - b)]$ (note that this implies $[(a^p - b^p)(a - b)]$ is a prime of the form $p^2k + 1$).

Based on data collected for $p = 3$, generalized versions of Propositions (35), (36), and (37) are true when $[(a^p - b^p)/(a - b)] = U^k$ where U is a prime and p does not divide k . (The propositions would be modified so that the modulus would be U instead of $[(a^p - b^p)/(a - b)]$.) This gives the following proposition;

(40) If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides a , b , $a - b$, or $a + b$, and $[(a^p - b^p)/(a - b)] = U^k$ where U is a prime and p does not divide k , then every factor of a , b , $a - b$, and $a + b$ is a p th power modulo U .

6 Wieferich's Criterion and the "pth Power with Respect to" Concept

In 1909, Wieferich [7] proved that if $a^p + b^p = c^p$, p does not divide abc , then $2p^{-1} \equiv 1 \pmod{p^2}$. Wieferich derived this criterion from very complicated formulas; a simpler approach is to employ the "pth power w.r.t." concept. The following proposition is based on data collected for $p = 3, 5, 7$, and 11;

(41) If $p > 3$, $q^{p-1} \not\equiv 1 \pmod{p^2}$, and q is a p th power w.r.t. $(a^p + b^p)/(a + b)$, then p divides a if q divides a , p divides b if q divides b , or p divides $a - b$ or

$a + b$ if q divides $a - b$ or $a + b$. If $p = 3$, $q^{p-1} \not\equiv 1 \pmod{p^2}$, and q is a p th power w.r.t. $(a^p + b^p)/(a + b)$, then p divides $a - b$ or $a + b$ if q divides $a - b$ or $a + b$.

This proposition precludes first-case solutions of Fermat's equation except when $2^{p-1} \equiv 1 \pmod{p^2}$ or $p = 3$ since $a^p + b^p = c^p$ implies $c^p + b^p$ divides $a^p + 2b^p$, $c^p + a^p$ divides $2a^p + b^p$, and $a^p - b^p$ divides $c^p - 2a^p$ and hence that 2 is a p th power w.r.t. $(c^p + b^p)/(c + b)$, $(c^p + a^p)/(c + a)$, and $(a^p - b^p)/(a - b)$. (If $a^p + b^p = c^p$, one of a , b , and c must be even.) Mirimanoff [8] proved that a first-case solution of Fermat's equation implies that $3^{p-1} \equiv 1 \pmod{p^2}$. The probability that a root of the congruence $x^{p-1} \equiv 1 \pmod{p^2}$, $0 < x < p^2$, is one larger than another root is $1/p$ (since there are $p - 1$ roots having $p(p - 1)$ possible values). There then shouldn't be any p such that $3^{p-1} \equiv 2^{p-1} \equiv 1 \pmod{p^2}$ since the sum of $(1/p)(1/p)$ over all p converges and the only p less than 3×10^9 such that $2^{p-1} \equiv 1 \pmod{p^2}$ are 1093 and 3511, and $3^{p-1} \not\equiv 1 \pmod{p^2}$ for either of these p .

Let ζ be a primitive p th root of unity and $K = Q(\zeta)$, a cyclotomic field of degree $p - 1$ over Q . Let λ denote $1 - \zeta$. The following proposition follows from the Chinese remainder theorem (and has also been confirmed using data collected for $p = 3$);

(42) q is a p th power w.r.t. $(a^p + b^p)/(a + b)$ if and only if q is congruent to the p th power of an integer modulo $a + \zeta b$, q is congruent to the p th power of an integer modulo $a + \zeta^2 b$, q is congruent to the p th power of an integer modulo $a + \zeta^3 b$, ..., and q is congruent to the p th power of an integer modulo $a + \zeta^{p-1} b$ (these are integers in K).

7 Barlow's Formulas and the "pth Power with Respect to" Concept

Barlow's formulas implied by a first-case solution of Fermat's equation are $(c^p - b^p)/(c - b) = R^p$, $(c^p - a^p)/(c - a) = S^p$, $(a^p + b^p)/(a + b) = T^p$, $c - b = r^p$, $c - a = s^p$, and $a + b = t^p$ where $rR = a$, $sS = b$, $tT = c$, and $\text{g.c.d.}(r, R) = \text{g.c.d.}(s, S) = \text{g.c.d.}(t, T) = 1$. Then a divides $S^p - c^{p-1}$ and $T^p - b^{p-1}$ and hence $c^{(f-1)/p} \equiv 1 \pmod{f}$ and $b^{(f-1)/p} \equiv 1 \pmod{f}$ for every prime factor f of R . (Note that $c^{(f-1)/p} \equiv b^{(f-1)/p} \pmod{f}$ and $c^p \equiv b^p \pmod{f}$ so that every prime factor of $(c^p - b^p)/(c - b)$ must be of the form $p^2k + 1$ [first proved by Sophie Germain [9]].) Analogous results hold for b and c . There can be first-case solutions of Fermat's equation only if c , b , and $c - b$ are p th powers w.r.t. $(c^p - b^p)/(c - b)$, c , a , and $c - a$ are p th powers w.r.t. $(c^p - a^p)/(c - a)$, a , b , and $a + b$ are p th powers w.r.t. $(a^p + b^p)/(a + b)$, and every prime factor of $(c^p - b^p)/(c - b)$, $(c^p - a^p)/(c - a)$, and $(a^p + b^p)/(a + b)$ is of the form $p^2k + 1$. Also, r divides $s^p - t^p$, s divides $r^p - t^p$, and t divides $r^p + s^p$. If

$n > 2$, $[(x^n + y^n)^{1/n} - x]^{1/n} + [(x^n + y^n)^{1/n} - y]^{1/n} > (x + y)^{1/n}$ where x and y are positive real numbers, therefore $r + s > t > r, s$ and hence each of r, s , and t has a prime factor of the form $pk + 1$. Also, $(a^p + b^p)/(a + b) = (a+b)(a^{p-2} - 2a^{p-3}b + 3a^{p-4}b^2 - \dots - (p-1)b^{p-2}) + pb^{p-1}$ so that $pb^{p-1} \equiv T^p \pmod{a + b}$.

Barlow's formulas implied by a second-case solution of Fermat's equation where p divides c are $(c^p - b^p)/(c - b) = R^p$, $(c^p - a^p)/(c - a) = S^p$, $(a^p + b^p)/(a + b) = pT^p$, $c - b = r^p$, $c - a = s^p$, and $a + b = (p^k t)^p/p$ where $rR = a$, $sS = b$, $p^k t T = c$, and $\text{g.c.d.}(r, R) = \text{g.c.d.}(s, S) = \text{g.c.d.}(p^k t, T) = 1$. Then c divides $R^p - b^{p-1}$ and $S^p - a^{p-1}$ and hence $b^{(f-1)/p} \equiv 1 \pmod{f}$ and $a^{(f-1)/p} \equiv 1 \pmod{f}$ for every prime factor f of T . Also, b divides $pT^p - a^{p-1}$ and $R^p - c^{p-1}$ and hence $(pa)^{(f-1)/p} \equiv 1 \pmod{f}$ and $c^{(f-1)/p} \equiv 1 \pmod{f}$ for every prime factor of S . Analogous results hold for a . There can be second-case solutions of Fermat's equation where p divides c only if c, pb , and $c - b$ are p th powers w.r.t. $(c^p - b^p)/(c - b)$, c, pa , and $c - a$ are p th powers w.r.t. $(c^p - a^p)/(c - a)$, a, b , and $p(a + b)$ are p th powers w.r.t. $(a^p + b^p)/(a + b)$, and every prime factor of $(a^p + b^p)/(a + b)/p$ is of the form $p^2k + 1$ (based on these formulas, the prime factors of $(c^p - b^p)/(c - b)$ and $(c^p - a^p)/(c - a)$ are not necessarily of the form $p^2k + 1$). (The requirement that every prime factor of $(a^p + b^p)/(a + b)/p$ be of the form $p^2k + 1$ could be said to be another characteristic property of the equation $a^p + b^p = c^p$, p divides c .) Also, p divides $a^{p-2} - 2a^{p-3}b + 3a^{p-4}b^2 - \dots - (p-1)b^{p-2}$ so that $b^{p-1} \equiv T^p \pmod{a + b}$ (this is relevant to fractional ideals to be discussed in the next section). The following proposition is based on data collected for $p = 3, 5, 7$, and 11 ;

(43) If $p > 3$, a is a p th power w.r.t. $(a^p + b^p)/(a + b)$, and p does not divide a , then $a^{p-1} \equiv 1 \pmod{p^2}$. If $p = 3$, a is a p th power w.r.t. $(a^p + b^p)/(a + b)$, and p divides b or $a - b$ or p^2 divides $a + b$, then $a^{p-1} \equiv 1 \pmod{p^2}$. Analogous results hold for b . If $a - b$ is a p th power w.r.t. $(a^p + b^p)/(a + b)$ and p does not divide $a - b$ or $a + b$, then $(a - b)^{p-1} \equiv 1 \pmod{p^2}$. Analogous results hold for $a + b$.

Proposition (43) shows that a second-case solution of Fermat's equation where p divides c implies $a^{p-1} \equiv 1 \pmod{p^2}$ and $b^{p-1} \equiv 1 \pmod{p^2}$ (avoiding the constraint that p not divide c in Furtwängler's first theorem).

8 Furtwängler's Theorems and Hasse's Reciprocity Law

This section requires some familiarity with algebraic number theory. In the following, parentheses sometimes denote the p th power residue symbol. Hasse [10] used one of his reciprocity laws to give a more systematic proof of Furtwängler's theorems. Hasse's reciprocity law is; $(\frac{\beta}{\alpha})(\frac{\alpha}{\beta})^{-1} = \zeta^{Tr(\eta)}$ where $\eta = \frac{\beta-1}{p} \cdot \frac{\alpha-1}{\lambda}$ for all α, β in $Q(\zeta)$ with $\text{g.c.d.}(\alpha, \beta) = 1$, $\alpha \equiv 1 \pmod{\lambda}$, $\beta \equiv 1 \pmod{p}$, and where

Tr denotes the trace from $Q(\zeta)$ to Q . Setting α to $(a+\zeta b)/(a+b)$ and β to q^{p-1} where q divides b gives $(\frac{q^{p-1}}{[(a+\zeta b)/(a+b)]}) = \zeta^{-u(p-1)b/(a+b)}$ where $u = (q^{p-1} - 1)/p$ (since $\alpha = 1 - \frac{b\lambda}{a+b} \equiv 1 \pmod{\lambda}$ and $\alpha \equiv 1 \pmod{q}$). If $a^p + b^p = c^p$, p does not divide c , then α is the p th power of an ideal and hence $(\frac{\beta}{\alpha}) = 1$ for all β in $Q(\zeta)$ that are prime to α . Then if p does not divide b , p must divide u .

The question of which of $(q^{p-1} - 1)/p$ and $a + b$ is divisible by the largest power of p can be avoided by considering the reciprocal of α . Let f_1 denote $\binom{1}{0}a^{p-2} - \binom{2}{1}a^{p-3}b + \binom{3}{2}a^{p-4}b^2 - \dots - \binom{p-1}{p-2}b^{p-2}$, f_2 denote $\binom{2}{0}a^{p-3} - \binom{3}{1}a^{p-4}b + \binom{4}{2}a^{p-5}b^2 - \dots + \binom{p-1}{p-3}b^{p-3}$, f_3 denote $\binom{3}{0}a^{p-4} - \binom{4}{1}a^{p-5}b + \binom{5}{2}a^{p-6}b^2 - \dots - \binom{p-1}{p-4}b^{p-4}$, ..., and f_{p-1} denote $\binom{p-1}{0}$. $\frac{a+\zeta^2 b}{a+\zeta b} \cdot \frac{a+\zeta^3 b}{a+\zeta^2 b} \cdots \frac{a+\zeta^{p-1} b}{a+\zeta^{p-2} b} = \frac{a+b}{a+\zeta b}$. Collecting terms in the product $(1 - \frac{b\lambda\zeta}{a+\zeta b})(1 - \frac{b\lambda\zeta^2}{a+\zeta^2 b}) \cdots (1 - \frac{b\lambda\zeta^{p-1}}{a+\zeta^{p-1} b})$ gives $\frac{a+b}{a+\zeta b} = 1 + (b\lambda f_1 + b^2\lambda^2 f_2 + \dots + b^{p-1}\lambda^{p-1} f_{p-1})/((a^p + b^p)/(a+b))$. $\text{Tr}(1) = p-1$ and $\text{Tr}(\lambda^k) = p$. Set α to $\frac{a+b}{a+\zeta b}$. Substituting for $\text{Tr}(1)$, $\text{Tr}(\lambda)$, $\text{Tr}(\lambda^2)$, ..., $\text{Tr}(\lambda^{p-2})$ and collecting terms gives $\text{Tr}((\alpha-1)/\lambda) = b((p-1)a^{p-2} - (p-2)a^{p-3}b + (p-3)a^{p-4}b^2 - \dots - b^{p-2})/((a^p + b^p)/(a+b))$. Setting β to q^{p-1} where q divides b gives $(\frac{q^{p-1}}{[(a+b)/(a+\zeta b)]}) = \zeta^{uv}$ where $v = b((p-1)a^{p-2} - (p-2)a^{p-3}b + (p-3)a^{p-4}b^2 - \dots - b^{p-2})/((a^p + b^p)/(a+b))$. If p divides $a + b$, then p also divides $(a^p + b^p)/(a+b)$. $(p-1)a^{p-2} - (p-2)a^{p-3}b + (p-3)a^{p-4}b^2 - \dots - b^{p-2}$ is congruent to $-(a+b)^{p-2}$ modulo p , therefore if p divides $a + b$, then $1/p$ does not divide v .

$p = (1-\zeta)(1-\zeta^2)(1-\zeta^3) \cdots (1-\zeta^{p-1})$ and the ideals $[1-\zeta]$, $[1-\zeta^2]$, $[1-\zeta^3]$, ..., $[1-\zeta^{p-1}]$ are equal. If p divides $a + b$ and $(a^p + b^p)/(a+b)/p$ is a p th power, then $\frac{(a+\zeta^2 b)/(1-\zeta^2)}{(a+\zeta b)/(1-\zeta)}$, $\frac{(a+\zeta^3 b)/(1-\zeta^3)}{(a+\zeta^2 b)/(1-\zeta^2)}$, $\frac{(a+\zeta^4 b)/(1-\zeta^4)}{(a+\zeta^3 b)/(1-\zeta^3)}$, ..., $\frac{(a+\zeta^{p-1} b)/(1-\zeta^{p-1})}{(a+\zeta^{p-2} b)/(1-\zeta^{p-2})}$ are p th powers of fractional ideals and hence $\frac{a+\zeta^2 b}{a+\zeta b}$, $\frac{a+\zeta^3 b}{a+\zeta^2 b}$, $\frac{a+\zeta^4 b}{a+\zeta^3 b}$, ..., $\frac{a+\zeta^{p-1} b}{a+\zeta^{p-2} b}$ are p th powers of fractional ideals. Furthermore, $\frac{a+\zeta^{i+1} b}{a+\zeta^i b} = 1 - \frac{b\lambda\zeta^i}{a+\zeta^i b} = \alpha_i \equiv 1 \pmod{\lambda}$, $i = 1, 2, 3, \dots, p-2$, and hence $(\frac{\beta}{\alpha_i}) = 1$ for all β in $Q(\zeta)$ that are prime to α_i . $\text{Tr}(\frac{-b\zeta}{a+\zeta b}) + \text{Tr}(\frac{-b\zeta^2}{a+\zeta^2 b}) + \text{Tr}(\frac{-b\zeta^3}{a+\zeta^3 b}) + \dots + \text{Tr}(\frac{-b\zeta^{p-1}}{a+\zeta^{p-1} b}) = b(a^{p-2} - 2a^{p-3}b + 3a^{p-4}b^2 - \dots - (p-1)b^{p-2})/((a^p + b^p)/(a+b))$, therefore if p divides $a+b$ and $(a^p + b^p)/(a+b)/p$ is a p th power, then $(\frac{q^{p-1}}{[(a+b)/(a+\zeta^{p-1} b)]}) = \zeta^{uw}$ where $w = b(a^{p-2} - 2a^{p-3}b + 3a^{p-4}b^2 - \dots - (p-1)b^{p-2})/((a^p + b^p)/(a+b))$. $a^{p-2} - 2a^{p-3}b + 3a^{p-4}b^2 - \dots - (p-1)b^{p-2}$ is congruent to $(a+b)^{p-2}$ modulo p , therefore $1/p$ does not divide w .

Let d , e , f , and g denote $(p-1)b^{p-2} - (p-2)b^{p-3}a + (p-3)b^{p-4}a^2 - \dots - a^{p-2}$, $(p-1)a^{p-2} - (p-2)a^{p-3}b + (p-3)a^{p-4}b^2 - \dots - b^{p-2}$, $a^{p-2} - 2a^{p-3}b + 3a^{p-4}b^2 - \dots - (p-1)b^{p-2}$, and $b^{p-2} - 2b^{p-3}a + 3b^{p-4}a^2 - \dots - (p-1)a^{p-2}$ respectively. Whether p^3 divides f or g is pertinent when 2 and p are split and p divides $a + b$. The following proposition is based on data collected for $p = 3$;

(44) If 2 divides b , p divides $a + b$, and $(a^p + b^p)/(a + b)/p$ is a p th power, then p^2 does not divide d (p^2 divides d when 2 divides a , etc.), p^2 divides e , p^2 does not divide f (p^3 divides f when 2 divides a , etc.), and p^3 divides g . Analogous results are valid for a . If $2p$ divides $a + b$ and $(a^p + b^p)/(a + b)/p$ is a p th power, then p^2 does not divide d , e , f or g .

The above proposition accounts for, in a systematic way, the form of the reformulated version of Furtwängler's theorems (at least, most of it). If 2 divides b , p divides $a + b$, $(a^p + b^p)/(a + b)/p$ is a p th power, and p^2 does not divide d , then whether p divides uv (where q divides a and u is defined to be $(q^{p-1} - 1)/p$) depends solely on u . However, $[\frac{a+b}{a+\zeta^{p-1}b}]$ is not a p th power of a fractional ideal in this case.

If 2 divides b , p divides $a + b$, $(a^p + b^p)/(a + b)/p$ is a p th power, and p^2 divides e , then p divides uv (where q divides b and u is defined to be $(q^{p-1} - 1)/p$). Again, $[\frac{a+b}{a+\zeta^{p-1}b}]$ is not a p th power of a fractional ideal.

If 2 divides b , p divides $a + b$, $(a^p + b^p)/(a + b)/p$ is a p th power, and p^2 does not divide f , then whether p divides uw (where q divides b and u is defined to be $(q^{p-1} - 1)/p$) depends solely on u . This allows for the possibility that $a/2$ is a p th power modulo p^2 (a provision of the reformulated version of Furtwängler's theorems). The origin of the condition that $a/2$ is a p th power modulo p^2 is unknown, but there should be some mechanism to account for the possibility that 2 is a p th power modulo p^2 and apparently this is it. By Proposition (43), if $p = 3$, a is a p th power w.r.t. $(a^p + b^p)/(a + b)$, and p^2 divides $a + b$, then a is a p th power modulo p^2 . This is not inconsistent with the reformulated version of Furtwängler's theorems since p^2 cannot divide $a + b$ when 2 does not divide $a + b$. However, if $p > 3$ and a is a p th power w.r.t. $(a^p + b^p)/(a + b)$, then a is a p th power modulo p^2 and hence 2 is a p th power modulo p^2 . By Barlow's formulas, if $a^p + b^p = c^p$ where p divides c , then a is a p th power w.r.t. $(a^p + b^p)/(a + b)$.

If 2 divides b , p divides $a + b$, $(a^p + b^p)/(a + b)/p$ is a p th power, and p^3 divides g , then p divides uw (where q divides a and u is defined to be $(q^{p-1} - 1)/p$). Then q is a p th power modulo p^2 .

The portion of the reformulated version of Furtwängler's theorems where 2 divides $a + b$ remains unaccounted for. The above proposition is also valid for multiples of 2, the multiples being factors of a , b , or $a + b$. When 2 and p are not split and 2 divides $a + b$, the multiples consist of powers of 2, powers of p , and products of primes that are usually not a p th power modulo p^2 .

9 Vandiver's Theorem

In 1919, Vandiver [11] proved that if $a^p + b^p = c^p$, p divides c , then p^3 divides c , $a^{p-1} \equiv 1 \pmod{p^3}$, and $b^{p-1} \equiv 1 \pmod{p^3}$. When a is odd, Vandiver's

theorem gives a necessary condition for a factor of a to be a p th power w.r.t. $(a^p + b^p)/(a + b)$ (based on data collected for $p = 3$). Analogous results hold for b , $a - b$, and $a + b$. The following proposition is based on data collected for $p = 3$;

(45) If $[(a^p + b^p)/(a + b)] = T^p$ and $T = U^k$ where U is a prime and p does not divide k , $2p$ divides a , b , $a - b$, or $a + b$, 2 does not divide a , q divides a , and $q^{p-1} \equiv 1 \pmod{p^3}$, then q is a p th power w.r.t. $(a^p + b^p)/(a + b)$. If $[(a^p + b^p)/(a + b)]$ is a p th power, $2p$ divides a , b , $a - b$, or $a + b$, 2 does not divide a , and q divides a , then q is a p th power w.r.t. $(a^p + b^p)/(a + b)$ only if $q^{p-1} \equiv 1 \pmod{p^3}$. Analogous results hold for b , $a - b$, and $a + b$. If $[(a^p + b^p)/(a + b)] = T^p$ and $T = U^k$ where U is a prime and p does not divide k , 2 divides a , p does not divide a , q divides a , and every prime factor of q is a p th power modulo p^2 , then q is a p th power w.r.t. $(a^p + b^p)/(a + b)$. Analogous results hold for b . If $[(a^p + b^p)/(a + b)] = T^p$ and $T = U^k$ where U is a prime and p does not divide k , p divides $a + b$, 2 does not divide $a + b$, q divides $a + b$, and $q^{p-1} \equiv 1 \pmod{p^3}$, then q is a p th power w.r.t. $(a^p + b^p)/(a + b)$. If $[(a^p + b^p)/(a + b)]$ is a p th power, p divides $a + b$, 2 does not divide $a + b$, q divides $a + b$, and p does not divide q , then q is a p th power w.r.t. $(a^p + b^p)/(a + b)$ only if $q^{p-1} \equiv 1 \pmod{p^3}$.

10 Euler's Theorem and "Split" 2 and p

Euler proved that every prime of the form $6k + 1$ can be represented by $x^2 + 3y^2$. Let T be a natural number and x , y , and z be integers. If $p = 3$, every prime factor of T is of the form $6k + 1$ and T has n such distinct prime factors, then T^p of pT^p has exactly pn representations of the form $(a^p + b^p)/(a + b)$. All representations of pT^p must be of the same type, that is, if $(a^p + b^p)/(a + b)$ is one representation, then p divides $a + b$, and if $((a')^p + (b')^p)/(a' + b')$ is another representation, then p must divide $a' + b'$. Representations of T^p can be of different types, that is, p can divide a , b , or $a - b$. Suppose $p = 3$, $(a^p + b^p)/(a + b)$ is a representation of pT^p , and 2 and p are common factors of $a + b$. When $p = 3$ and $x + y = z$, $(x^p - y^p)/(x - y) = (z^p + y^p)/(z + y) = (z^p + x^p)/(z + x)$, so 2 must divide b' where $b' = a - b$ and $a' = a$ for the representation $((a')^p + (b')^p)/(a' + b')$ of pT^p (and p must divide $a' + b'$) and 2 must divide a'' where $a'' = a - b$ and $b'' = -b$ for the representation $((a'')^p + (b'')^p)/(a'' + b'')$ of pT^p (and p must divide $a'' + b''$).

11 A Generalization of Vandiver's Theorem

There is some evidence that if there is one representation $[(a^p + b^p)/(a + b)]$ of T^p for $p > 3$, there must be other representations. If $a^p + b^p = c^p$, p divides c , and every prime factor of $(c^p - b^p)/(c - b)$ and $(c^p - a^p)/(c - a)$ is of the form

$p^2k + 1$, then p^3 divides c by Barlow's formulas (since $a^p + b^p + a + b - 2c = r^p(R^p - 1) + s^p(S^p - 1)$). Vandiver's theorem suggests that no prime factor of $(c^p - b^p)/(c - b)$ or $(c^p - a^p)/(c - a)$ can just be of the form $pk + 1$. Vandiver's theorem can be reformulated so that it is applicable to the problem of determining if $[(a^p + b^p)/(a + b)]$ can be a p th power. The following proposition is based on data collected for $p = 3$;

(46) If $[(a^p + b^p)/(a + b)] = T^p$ where every prime factor of T is of the form $p^2k + 1$, p^3 divides a , b , or $a - b$ or p^4 divides $a + b$, and 2 does not divide a , then $a^{p-1} \equiv 1 \pmod{p^3}$. If $[(a^p + b^p)/(a + b)] = T^p$ where T has only one distinct prime factor, this prime factor is of the form $p^2k + 1$, p^3 divides a , b , or $a - b$ or p^4 divides $a + b$ or p^3 divides a' , b' , or $a' - b'$ or p^4 divides $a' + b'$ for some representation $[((a')^p + (b')^p)/(a' + b')]$ of T^p , and 2 does not divide a , then $a^{p-1} \equiv 1 \pmod{p^3}$. Analogous results hold for b and $a - b$. If $[(a^p + b^p)/(a + b)] = T^p$ where every prime factor of T is of the form $p^2k + 1$, p^3 divides a , b , or $a - b$ or p^4 divides $a + b$, and 2 does not divide $a + b$, then $[(a + b)/p]^{p-1} \equiv 1 \pmod{p^3}$ if p divides $a + b$, or $(a + b)^{p-1} \equiv 1 \pmod{p^3}$ if p does not divide $a + b$. If $[(a^p + b^p)/(a + b)] = T^p$ where T has only one distinct prime factor, this prime factor is of the form $p^2k + 1$, p^3 divides a , b , or $a - b$ or p^4 divides $a + b$ or p^3 divides a' , b' , or $a' - b'$ or p^4 divides $a' + b'$ for some representation $[((a')^p + (b')^p)/(a' + b')]$ of T^p , and 2 does not divide $a + b$, then $[(a + b)/p]^{p-1} \equiv 1 \pmod{p^3}$ if p divides $a + b$, or $(a + b)^{p-1} \equiv 1 \pmod{p^3}$ if p does not divide $a + b$. If $[(a^p + b^p)/(a + b)] = T^p$ where every prime factor of T is of the form $p^2k + 1$, 2 divides a , and p does not divide a , then $(a/2)^{p-1} \equiv 1 \pmod{p^3}$. Analogous results hold for b . If $[(a^p + b^p)/(a + b)] = T^p$ where every prime factor of T is of the form $p^2k + 1$, 2 does not divide a , and p divides $a + b$, then $a^{p-1} \equiv 1 \pmod{p^3}$. Analogous results hold for b and $a - b$.

12 Congruence Properties of Prime Factors of $[(a^p + b^p)/(a + b)]$ when $[(a^p + b^p)/(a + b)]$ is a p th Power

That the reformulation of Vandiver's theorem depends on different representations of $[(a^p + b^p)/(a + b)]$ of T^p is some indication that different representations must exist for $p > 3$ (if there are any representations). Whether p is a p th power w.r.t. $(a^p + b^p)/(a + b)$ is of importance to Vandiver's theorem. The following propositions are based on data collected for $p = 3$;

(47) If $[(a^p + b^p)/(a + b)] = T^p$ and $T = U^k$ where U is a prime and p does not divide k , then p is a p th power w.r.t. $(a^p + b^p)/(a + b)$ if and only if p^3 divides a , b , or $a - b$ or p^4 divides $a + b$ or p^3 divides a' , b' or $a' - b'$ or p^4 divides $a' + b'$ for some representation $[((a')^p + (b')^p)/(a' + b')]$ of T^p . If $[(a^p + b^p)/(a + b)] = T^p$ and $T = U^k$ where U is a prime and p divides k ,

then p is not a p th power w.r.t. $(a^p + b^p)/(a + b)$. If $[(a^p + b^p)/(a + b)] = T^p$ where T has two distinct prime factors, $2p$ divides a , b , $a - b$, or $a + b$, and p is a p th power w.r.t. $(a^p + b^p)/(a + b)$, then p^3 divides a , b , or $a - b$ or p^4 divides $a + b$.

(48) If $[(a^p + b^p)/(a + b)]$ is a p th power, then $p^{p-1}a$ is a p th power w.r.t. $(a^p + b^p)/(a + b)$ if $2p$ divides a , $p^{p-1}b$ is a p th power w.r.t. $(a^p + b^p)/(a + b)$ if $2p$ divides b , $p^{p-1}(a - b)$ and $a + b$ are p th powers w.r.t. $(a^p + b^p)/(a + b)$ if $2p$ divides $a - b$, or $a - b$ and $p(a + b)$ are p th powers w.r.t. $(a^p + b^p)/(a + b)$ if $2p$ divides $a + b$.

(49) If $[(a^p + b^p)/(a + b)]$ is a p th power, 2 divides a , and p does not divide a , then a is a p th power w.r.t. $(a^p + b^p)/(a + b)$. Analogous results hold for b .

(50) If $[(a^p + b^p)/(a + b)]$ is a p th power, f is a prime factor of $[(a^p + b^p)/(a + b)]$ of the form $p^2k + 1$, and p is not a p th power modulo f , then (1) $p^{p-1}a$, $p^{p-1}b$, $p^{p-1}(a - b)$, and $a + b$ are p th powers modulo f if p divides a , b , or $a - b$, or (2) a , b , $a - b$, and $p(a + b)$ are p th powers modulo f if p divides $a + b$. If $[(a^p + b^p)/(a + b)]$ is a p th power, f is a prime factor of $[(a^p + b^p)/(a + b)]$ of the form $p^2k + 1$, and p is a p th power modulo f , then a , b , $a - b$, and $a + b$ are p th powers modulo f .

(51) If $[(a^p + b^p)/(a + b)]$ is a p th power, f is a prime factor of $[(a^p + b^p)/(a + b)]$ not of the form $p^2k + 1$, and p is not a p th power modulo f , then (1) $p^{p-1}a$, b , $p(a - b)$, and $p^{p-1}(a + b)$, or $p^{p-1}a$, pb , $a - b$, and $p(a + b)$ are p th powers modulo f if $2p$ divides a , or (2) a , $p^{p-1}b$, $p(a - b)$, and $p^{p-1}(a + b)$, or pa , $p^{p-1}b$, $a - b$, and $p(a + b)$ are p th powers modulo f if $2p$ divides b , or (3) a , pb , $p^{p-1}(a - b)$, and $a + b$, or pa , b , $p^{p-1}(a - b)$, and $a + b$ are p th powers modulo f if $2p$ divides $a - b$, or (4) pa , $p^{p-1}b$, $a - b$, and $p(a + b)$, or $p^{p-1}a$, pb , $a - b$, and $p(a + b)$ are p th powers modulo f if $2p$ divides $(a + b)$.

(52) If $[(a^p + b^p)/(a + b)]$ is a p th power, 2 divides a , p does not divide a , f is a prime factor of $[(a^p + b^p)/(a + b)]$ not of the form $p^2k + 1$, and p is not a p th power modulo f , then a , pb , $p^{p-1}(a - b)$, and $a + b$, or a , $p^{p-1}b$, $p(a - b)$, and $p^{p-1}(a + b)$ are p th powers modulo f . Analogous results hold for b .

Since Propositions (48), (50), (51), and (52) are based solely on data collected for $p = 3$, their form is ambiguous in that the p exponents might be 2 instead of $p - 1$. Congruence properties of the prime factors of $[(a^p - b^p)/(a - b)]$ when $[(a^p + b^p)/(a + b)]$ is a p th power appear to determine the form of Propositions (48), (50), (51), and (52). (Propositions (48), (50), (51), and (52) can be transformed into Propositions (12), (8), (14), and (9) respectively by multiplying the a , b , $a - b$, and $a + b$ terms by p and switching the $a + b$ and $a - b$ terms [and of course the moduli bases]. This is just an attempt to find a simple relationship between the congruence properties of the prime factors of $[(a^p + b^p)/(a + b)]$ and $[(a^p - b^p)/(a - b)]$ when $[(a^p + b^p)/(a + b)]$ is a p th power and has no apparent logical basis.)

(53) If $[(a^p + b^p)/(a + b)]$ is a p th power, f is a prime factor of $[(a^p + b^p)/(a + b)]$ not of the form $p^2k + 1$, and p is a p th power modulo f , then (1) a (and not b , $a - b$, or $a + b$) is a p th power modulo f if 2 divides a , or (2) b (and not a , $a - b$ or $a + b$) is a p th power modulo f if 2 divides b , or (3) $a - b$ and $a + b$ (and not a or b) are p th powers modulo f if 2 divides $a - b$ or $a + b$.

As shown previously, $a^p + b^p = c^p$, p divides c , implies c , pb , and $c - b$ are p th powers w.r.t. $(c^p - b^p)/(c - b)$, c , pa , and $c - a$ are p th powers w.r.t. $(c^p - a^p)/(c - a)$, and 2 and p are common factors of c (if the reformulated version of Furtwängler's theorem is accepted). Then by Propositions (51) and (53), every prime factor of $(c^p - b^p)/(c - b)$ and $(c^p - a^p)/(c - a)$ must be of the form $p^2k + 1$. (Substituting c for a and $-b$ for b in Proposition (51) gives $p^{p-1}c$, $-b$, $p(c + b)$, and $p^{p-1}(c - b)$, or $p^{p-1}c$, $-pb$, $c + b$ and $p(c - b)$ are p th powers modulo f [a prime factor of $(c^p - b^p)/(c - b)$] if $2p$ divides c and p is not a p th power modulo f [a contradiction]. Substituting c for a and $-b$ for b in Proposition (53) gives c [and not $c - b$] is a p th power modulo f if $2p$ divides c and p is a p th power modulo f [a contradiction]. Analogous results follow by substituting c for a and $-a$ for b in Propositions (51) and (53). Furthermore, by Proposition (50), p must be a p th power w.r.t. $(c^p - b^p)/(c - b)$ and $(c^p - a^p)/(c - a)$. As shown previously, $a^p + b^p = c^p$, p divides c , implies a , b , and $p(a + b)$ are p th powers w.r.t. $(a^p + b^p)/(a + b)$ and every prime factor of $[(a^p + b^p)/(a + b)]$ is of the form $p^2k + 1$. This gives the following proposition;

(54) If $a^p + b^p = c^p$ where p divides c , then every prime factor of $(c^p - b^p)/(c - b)$ is of the form $p^2k + 1$ and c , b , $c - b$, $c + b$, and p are p th powers w.r.t. $(c^p - b^p)/(c - b)$. Analogous results hold for $(c^p - a^p)/(c - a)$. If $a^p + b^p = c^p$ where p divides c , then every prime factor of $[(a^p + b^p)/(a + b)]$ is of the form $p^2k + 1$ and a , b , $a - b$, and $p(a + b)$ are p th powers w.r.t. $(a^p + b^p)/(a + b)$.

More evidence for the above proposition is given by the following three propositions (based on data collected for $p = 3, 5$, and 7);

(55) If every prime factor of $[(a^p + b^p)/(a + b)]$ is of the form $p^2k + 1$ and p^2 divides a , b , $a - b$, or $a + b$, then $a^{p-1} \equiv 1 \pmod{p^2}$ if p does not divide a , $b^{p-1} \equiv 1 \pmod{p^2}$ if p does not divide b , and $(a - b)^{p-1} \equiv 1 \pmod{p^2}$ and $(a + b)^{p-1} \equiv 1 \pmod{p^2}$ if p does not divide $a - b$ or $a + b$.

(56) If a , pb , and $a + b$ are p th powers w.r.t. $(a^p + b^p)/(a + b)$ and p^2 divides a , then b , $a + b$, and $a - b$ are p th powers modulo p^2 . If $p = 3$ or 5 , a , pb , and $a + b$ are p th powers w.r.t. $(a^p + b^p)/(a + b)$, and p^2 divides a , b , $a - b$, or $a + b$, then $a - b$ is a p th power w.r.t. $(a^p + b^p)/(a + b)$ if and only if p is a p th power w.r.t. $(a^p + b^p)/(a + b)$.

(57) If a , b , and $p(a + b)$ are p th powers w.r.t. $(a^p + b^p)/(a + b)$ and p^2 divides a or b , then $a + b$ and $a - b$ are p th powers modulo p^2 . If $p = 3$, a , b , and $p(a + b)$

are p th powers w.r.t. $(a^p + b^p)/(a + b)$, and p^2 divides a , b , $a - b$, or $a + b$, then $a - b$ is a p th power w.r.t. $(a^p + b^p)/(a + b)$.

Substituting c for a and $-b$ for b in Proposition (14) gives $p^2(c - b)$ is a p th power modulo f (a prime factor of $(c^p + b^p)/(c + b)$ not of the form $p^2k + 1$) if $2p$ divides c and $p/2$ is a p th power modulo f , or $p(c - b)$ is a p th power modulo f if $2p$ divides c and $2p$ is a p th power modulo f . Then if $c - b$ is a p th power, p must be a p th power modulo f and hence by Proposition (7), 2 cannot be a p th power modulo f (otherwise, $2p$ would be a p th power modulo f). As shown previously, $a^p + b^p = c^p$ implies 2 is a p th power w.r.t. $(c^p + b^p)/(c + b)$. This gives the following proposition;

(58) If $a^p + b^p = c^p$ where p divides c , then every prime factor of $(c^p + b^p)/(c + b)$ is of the form $p^2k + 1$ and c , b , $p(c + b)$, and $c - b$ are p th powers w.r.t. $(c^p + b^p)/(c + b)$. Analogous results hold for $(c^p + a^p)/(c + a)$.

The following proposition is based on data collected for $p = 3$;

(59) If $[(a^p + b^p)/(a + b)]$ is a p th power and f is a prime factor of $[(a^p + b^p)/(a + b)]$, then at least one of $2p$, 2, p , or $p/2$ is a p th power modulo f .

The following propositions are based on data collected for $p = 3, 5$, and 7;

(60) If p is a p th power w.r.t. $(a^p + b^p)/(a + b)$, then p^2 divides a if p divides a , p^2 divides b if p divides b , or p^2 divides $a - b$ if p divides $a - b$. If $p > 3$ and p is a p th power w.r.t. $(a^p + b^p)/(a + b)$, then p^2 divides $a + b$ if p divides $a + b$. If $p = 3$ and p is a p th power w.r.t. $(a^p + b^p)/(a + b)$, then p^3 divides $a + b$ if p^2 divides $a + b$.

When p is a p th power w.r.t. $(a^p + b^p)/(a + b)$ and $[(a^p + b^p)/(a + b)]$ is not prime, the ‘‘small’’ prime factors of $[(a^p + b^p)/(a + b)]$ are not of the form $p^2k + 1$. For example, of the 2,517 prime factors (not necessarily distinct) of $[(a^p + b^p)/(a + b)]$ for the 1,175 (a, b) such that p is a p th power w.r.t. $(a^p + b^p)/(a + b)$, $[(a^p + b^p)/(a + b)]$ is not prime, and $1,000 \geq a > b \geq 1$ for $p = 7$, only 214 prime factors are of the form $p^2k + 1$ and the smallest of these prime factors is 15,877. When $p = 3$ and p is a p th power w.r.t. $(a^p + b^p)/(a + b)$, the three smallest prime factors of $[(a^p + b^p)/(a + b)]$ of the form $p^2k + 1$ are 73, 271, and 307.

(61) If $p = 3$, a , b , $a - b$, and $a + b$ are p th powers w.r.t. $(a^p + b^p)/(a + b)$, p^2 divides a , b , $a - b$, or $a + b$, and $[(a^p + b^p)/(a + b)]$ is not prime, then every prime factor of $[(a^p + b^p)/(a + b)]$ equals $[(a')^p + (b')^p]/(a' + b')$ where p^2 divides a' , b' , $a' - b'$, or $a' + b'$. (The smallest prime factor of $[(a^p + b^p)/(a + b)]$ satisfying these conditions is 73; the requirement that p^2 divide a' , b' , $a' - b'$, or $a' + b'$ eliminates about $\frac{2}{3}$ of the primes of the form $p^2k + 1$ from consideration.)

For the 13,208,764 (a, b) such that $50,000 \geq a > b \geq 1$, a , b , $a - b$, and $a + b$ are p th powers w.r.t. $(a^p + b^p)/(a + b)$, and p^2 divides a , b , $a - b$, or $a + b$

for $p = 3$, the numbers of instances where $[(a^p + b^p)/(a + b)]$ has 1, 2, 3, and 4 prime factors (not necessarily distinct) are 12,585,008, 615,167, 8,518, and 71 respectively. $[(a^p + b^p)/(a + b)]$ is a square in 624 instances, a cube in 27 instances, and a fourth power in 3 instances. For larger upper bounds of the a , b values, the proportions of the numbers of instances where $[(a^p + b^p)/(a + b)]$ has 2, 3, and 4 prime factors increase, so there should eventually be a value of $[(a^p + b^p)/(a + b)]$ having 5 or more prime factors.

(62) If $p = 3$, a , b , $a - b$, and $p(a + b)$ are p th powers w.r.t. $(a^p + b^p)/(a + b)$, p is not a p th power w.r.t. $(a^p + b^p)/(a + b)$, p^2 divides a , b , $a - b$, or $a + b$, and $[(a^p + b^p)/(a + b)]$ is not prime, then every prime factor of $[(a^p + b^p)/(a + b)]$ equals $[((a')^p + (b')^p)/(a' + b')]$ where p^2 does not divide a' , b' , $a' - b'$, or $a' + b'$.

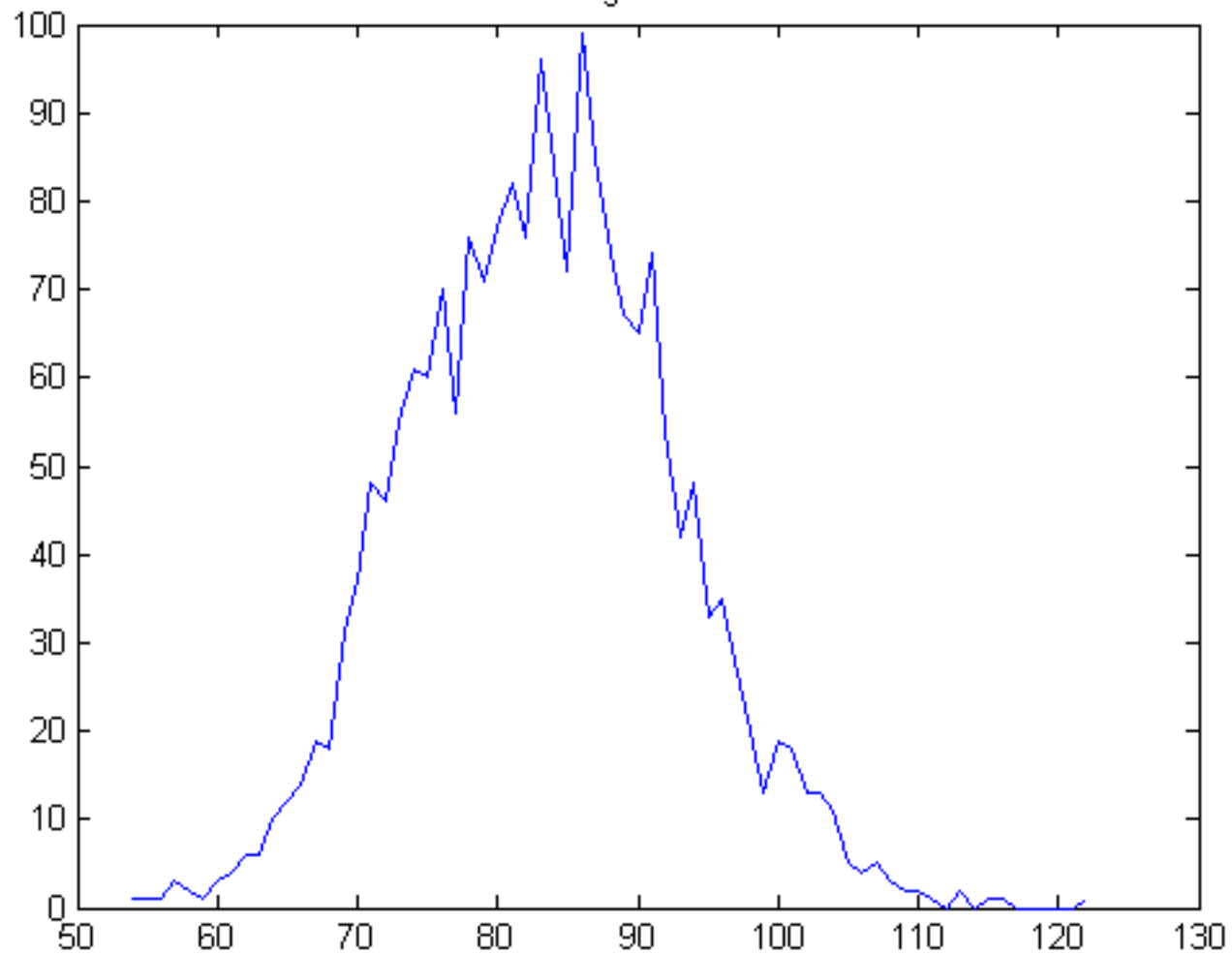
For the 1,316,973 (a, b) such that $25,000 \geq a > b \geq 1$, a , b , $a - b$, and $p(a + b)$ are p th powers w.r.t. $(a^p + b^p)/(a + b)$, p is not a p th power w.r.t. $(a^p + b^p)/(a + b)$, and p^2 divides a , b , $a - b$, or $a + b$ for $p = 3$, the numbers of instances where $[(a^p + b^p)/(a + b)]$ has 1, 2, 3, 4, 5, and 6 prime factors are 712,815, 573,912, 29,149, 1,002, 88, and 7 respectively. $[(a^p + b^p)/(a + b)]$ is a square in 112 instances, a cube in 9 instances, and a fourth power in 2 instances.

If $p = 5$, $5,000 \geq a > b \geq 1$, a , b , $a - b$, and $a + b$ are p th powers w.r.t. $(a^p + b^p)/(a + b)$, and p^2 divides a , b , $a - b$, or $a + b$, then $[(a^p + b^p)/(a + b)]$ has at most two prime factors. If $p = 7$, $500 \geq a > b \geq 1$, a , b , $a - b$, and $a + b$ are p th powers w.r.t. $(a^p + b^p)/(a + b)$, and p^2 divides a , b , $a - b$, or $a + b$, then $[(a^p + b^p)/(a + b)]$ is prime. If $p = 5$, $5,000 \geq a > b \geq 1$, a , b , $a - b$, and $p(a + b)$ are p th powers w.r.t. $(a^p + b^p)/(a + b)$, p is not a p th power w.r.t. $(a^p + b^p)/(a + b)$, and p^2 divides a , b , $a - b$, or $a + b$, then $[(a^p + b^p)/(a + b)]$ has at most three prime factors. If $p = 7$ and $500 \geq a > b \geq 1$, there do not exist (a, b) such that a , b , $a - b$, and $p(a + b)$ are p th powers w.r.t. $(a^p + b^p)/(a + b)$, p is not a p th power w.r.t. $(a^p + b^p)/(a + b)$, and p^2 divides a , b , $a - b$, or $a + b$. For $p = 5$, the prime factors of $[(a^p + b^p)/(a + b)]$ when a , b , $a - b$, and $a + b$ are p th powers w.r.t. $(a^p + b^p)/(a + b)$ and p^2 divides a , b , $a - b$, or $a + b$ are different from the prime factors of $[(a^p + b^p)/(a + b)]$ when a , b , $a - b$, and $p(a + b)$ are p th powers w.r.t. $(a^p + b^p)/(a + b)$, p is not a p th power w.r.t. $(a^p + b^p)/(a + b)$, and p^2 divides a , b , $a - b$, or $a + b$, the same as for $p = 3$. For $p = 3$, this was due to the representations of the prime factors. For $p = 5$ and $5,000 \geq a > b \geq 1$, there are 25,287 prime values of $[(a^p + b^p)/(a + b)]$ where a , b , $a - b$, and $a + b$ are p th powers w.r.t. $(a^p + b^p)/(a + b)$ and p^2 divides a , b , $a - b$ or $a + b$. For $p = 5$ and $5,000 \geq a > b \geq 1$, there are no prime values of $[(a^p + b^p)/(a + b)]$ where a , b , $a - b$, and $p(a + b)$ are p th powers w.r.t. $(a^p + b^p)/(a + b)$, p is not a p th power w.r.t. $(a^p + b^p)/(a + b)$, and p^2 divides a , b , $a - b$, or $a + b$. This is some indication that representations (of the form $[(a^p + b^p)/(a + b)]$) of the prime factors are still relevant for $p > 3$.

References

- [1] P. Barlow, *Demonstration of a curious numerical proposition*, J. Nat. Phil. Chem. and Arts, 27, 1810, 193-205
- [2] P. Furtwängler, *Letzter Fermatschen Satz und Eisensteins'ches Reziprozitätsgesetz*, Sitzungsber, Akad. d. Wiss. Wein., Abt. IIa, 121, 1912, 589-592
- [3] F. Diamond and J. Shurman, *A First Course in Modular Forms*, Springer, 2005
- [4] J. Shurman, "<http://people.reed.edu/~jerry//MF/talk.pdf>"
- [5] L. Mordell, *On the rational solutions of the indeterminate equation of the third and fourth degree*, Proc. Cambridge Philos. Soc., 21, 1922, 179-193
- [6] G. Faltings, *Endlichkeits sätze für abelsche varietäten über zahlkörpern*, Inventiones Mathematicae, 73(3), 1983, 349-366
- [7] A. Wieferich, *Zum Letzten Fermat'schen Theorem*, J. reine u. angew. Math. 136, 1909, 293-302
- [8] D. Mirimanoff, *Sur le dernier théorème de Fermat*, J. reine u. angew. Math. 139, 1911, 309-324
- [9] A. M. Legendre, *Sur quelques objets d'analyse indéterminée et particulièrement sur le théorème de Fermat*, Mém. Acad. R. Sc. de l'Institut de France, 6, année 1823, Paris, 1827, 1-60. (Results are attributed to Sophie Germain in a footnote.)
- [10] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Teil I: Klassenkörpertheorie. Teil Ia: Beweise zu Teil I; Teil II: Reziprozitätsgesetz. 3. Aufl.. Würzburg Wien: Physika-Verlag. 204 pp. Jbuch 52-150; 53, 143; 46-165, 1970
- [11] H. S. Vandiver, *A property of cyclotomic integers and its relation to Fermat's last theorem*, Annals of Math., 21, 1919, 73-80

Figure 1



Normal Probability Plot

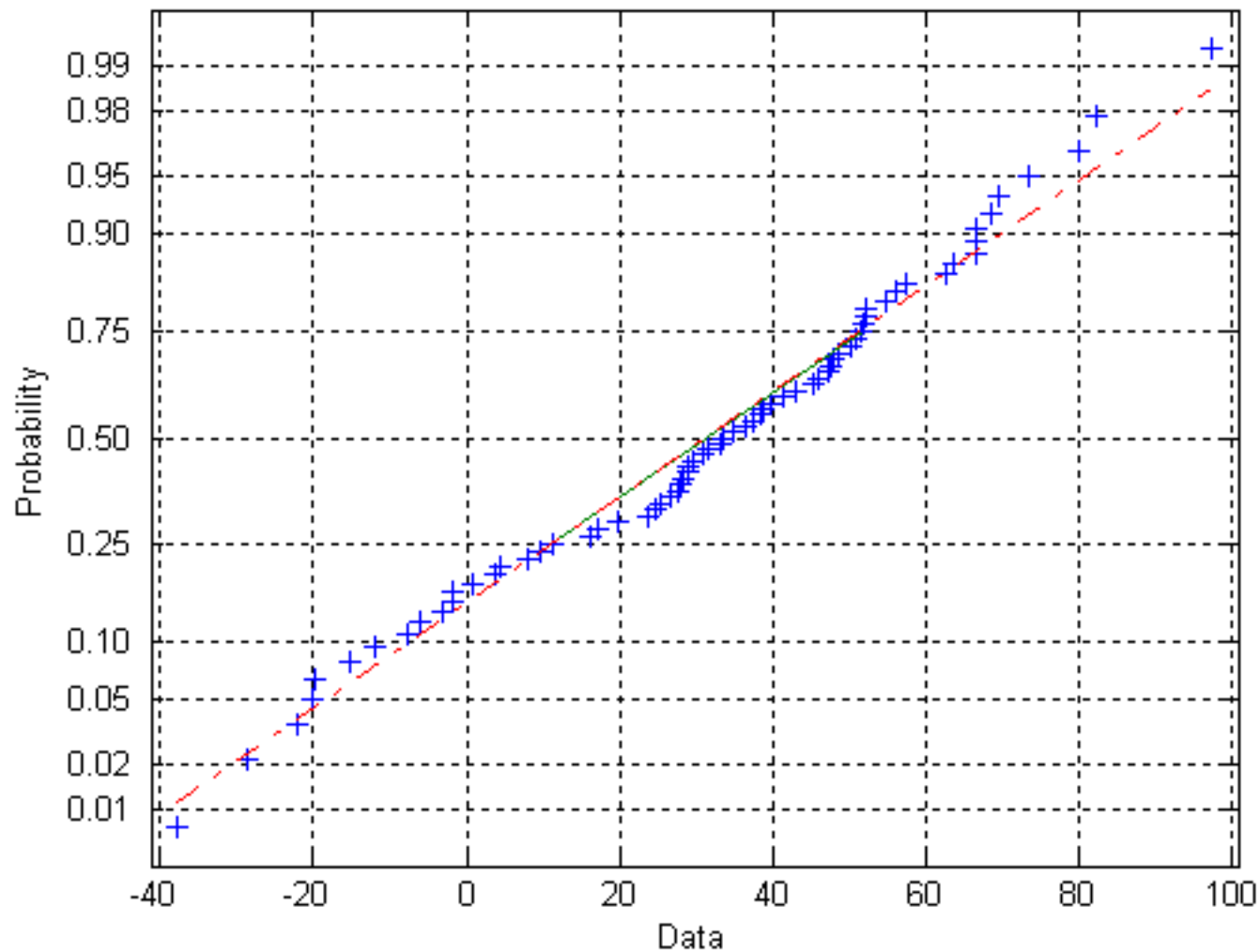
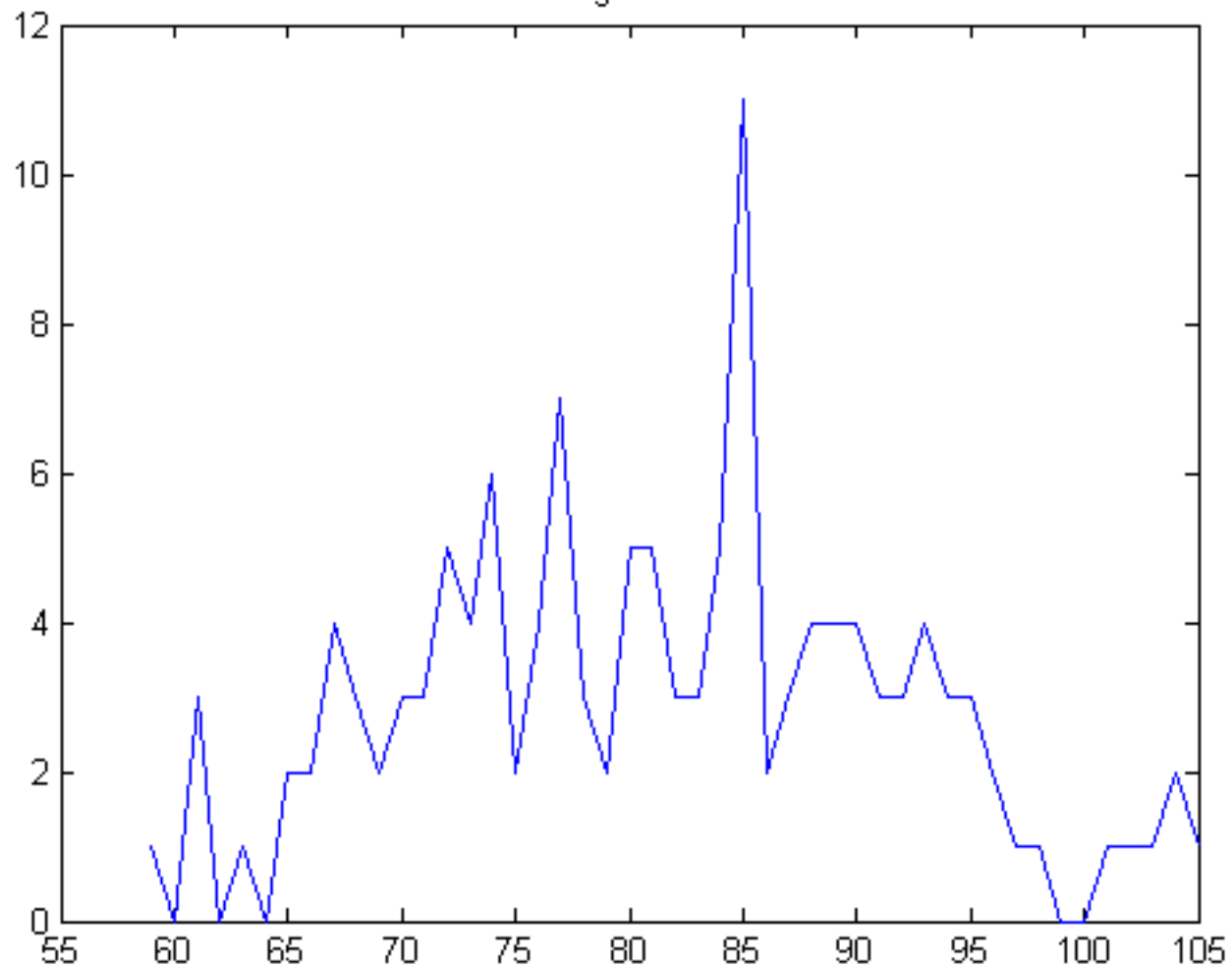


Figure 3



Normal Probability Plot

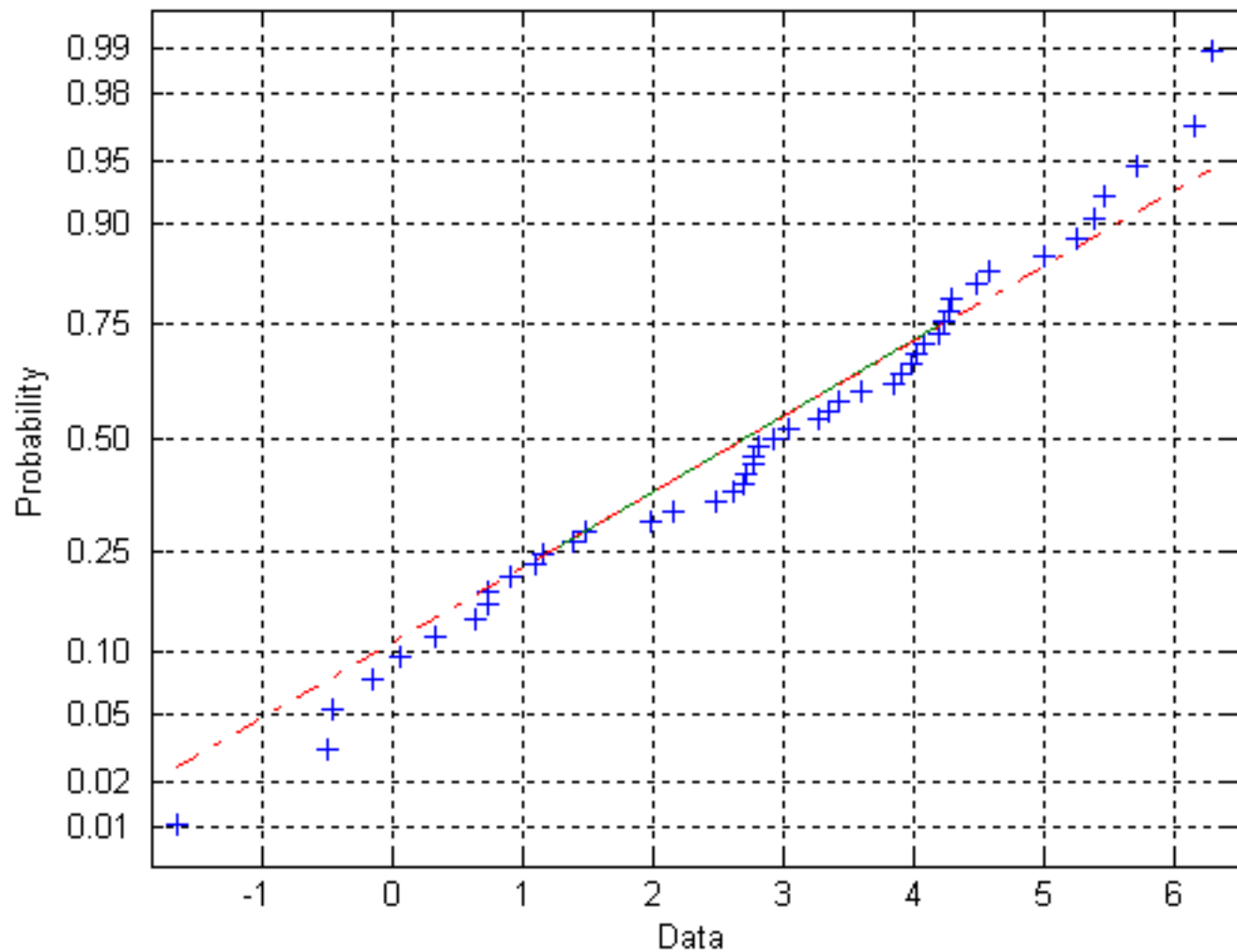
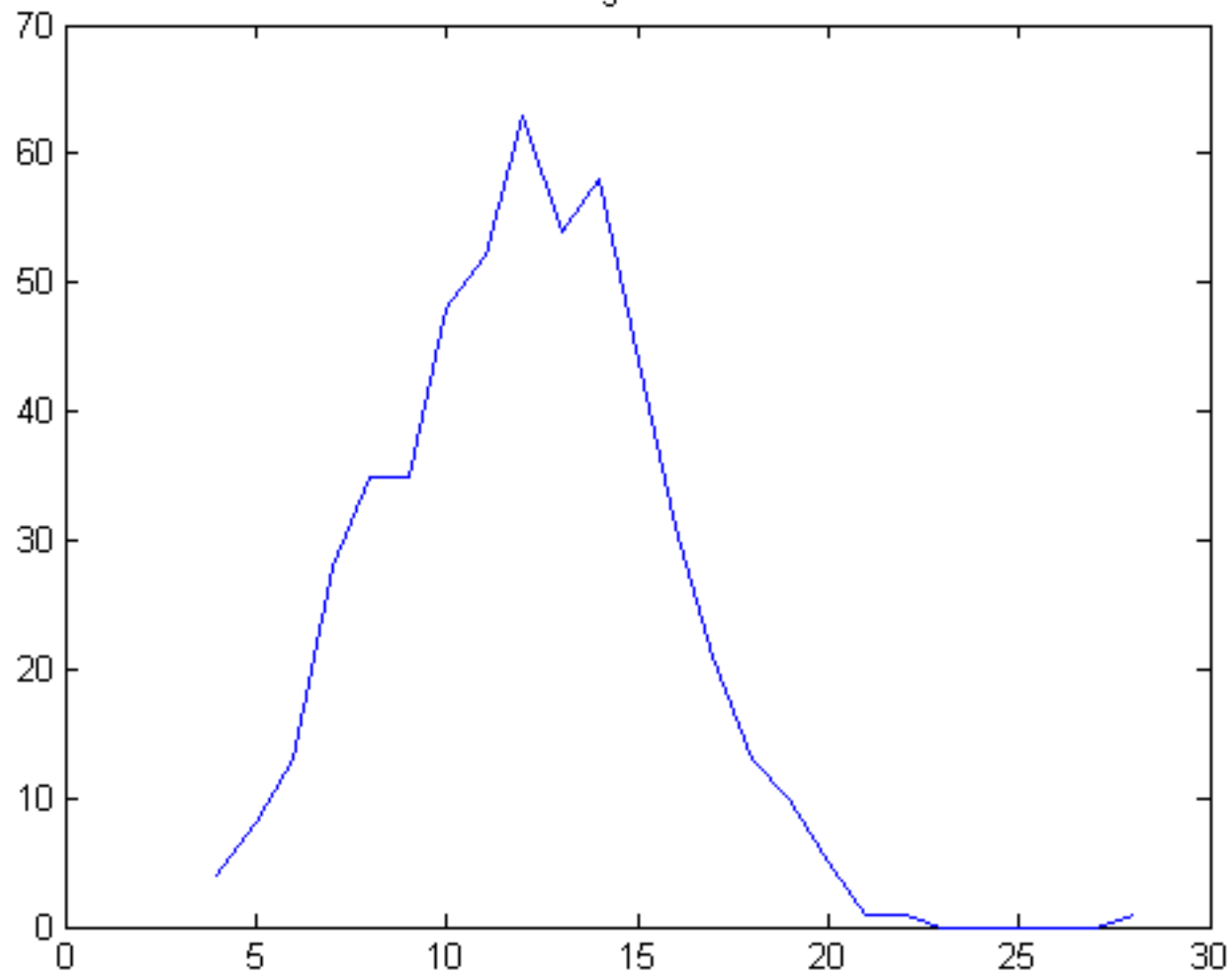


Figure 5



Normal Probability Plot

