

CHAPTER II

Prime number, factorisation and divisibility theorems

2.1. Introduction.

We obtain primality conditions not dealt with in most textbooks, e.g. for ‘*generalised Fermat*’ numbers, for positive natural numbers γ or $\delta > 1$ and p , we prove that no number of the form $\gamma^p + \delta^p$ is prime, except for the possibilities $p = 1$ or p a power of 2.

For ‘*generalised Mersenne*’ numbers, no representations of primes are of the form $\gamma^p - \delta^p$, except for the possibilities $p = 1$, or $\delta = (\gamma - 1)$ and p prime.

We also discuss a linear combination of powers prime number theorem and continue with a discussion on factorisation of p th powers $\gamma^p \pm \delta^p$.

This chapter also discusses extensions of *Fermat’s little theorem*, including theorems connected with *reciprocity*. We make some remarks on *Fermat’s last theorem*.

2.2 Prime number theorems.

For γ or $\delta > 1 \in \mathbf{N}$, no representations of primes are of the form

$$\gamma^p + \delta^p,$$

except for the possibilities $p = 1$ or p a power of 2, the latter subsumed under $p = 2$.

Proof. Let p be odd. Then by (**), supposing the above expression is prime

$$\begin{aligned} \gamma \uparrow (p^m) + \delta \uparrow (p^m) &= [\gamma + \delta] \Pi(r = 0, m - 1) \\ &\{ \Sigma(s = 0, p - 1)[(\gamma \uparrow [p^{m-1-r}]) \uparrow s][((-\delta) \uparrow [p^{m-1-r}]) \uparrow (p - 1 - s)] \}. \end{aligned}$$

Since the prime number and $\gamma + \delta$ are positive, so is the subsequent expression in [] which is a summation of integers, and $m = 1$, otherwise the expression factorises. Since $\gamma + \delta > 1$, the summation of integers is 1. This implies

$$\gamma^p + \delta^p = \gamma + \delta,$$

which is clearly only the case for $\gamma = \delta = 1$ or $p = 1$. Hence if $p \neq 1$, it is not odd.

Now if $p \neq 1$ is not a power of 2, there exists an odd factor $q \neq 1$ so that $p = kq$ and

$$(\gamma \uparrow k) \uparrow q + (\delta \uparrow k) \uparrow q$$

is prime, which we have proved is not the case. Hence $p = 1$, or $p = 2z$ is a power of 2, so all the latter such primes can be written as

$$(\gamma \uparrow z) \uparrow 2 + (\delta \uparrow z) \uparrow 2. \blacksquare$$

We note the following standard results, given e.g. in [3].

No prime of the form $4k + 3$ is a sum of two squares. ■

Any prime of the form $4k + 1$ can be represented uniquely (aside from the order of summands) as a sum of two squares. ■

2.3 Factorisation theorems.

Let p be odd, $\eta \neq \pm\theta \neq 0$ be integers, $\gamma \neq \delta \neq 0$ natural numbers,

$$X = \Sigma(s = 0, p - 1)[\gamma^s][(-\delta)^{p-1-s}],$$

$$Y = \Sigma(s = 0, p - 1)[\gamma^s][\delta^{p-1-s}]$$

and

$$Z = \eta(\gamma^p) + \theta(\delta^p) > 0.$$

If the product of $(\eta + \theta)$, $(\gamma + \delta)$ and X has two prime factors in common with the product $(\eta - \theta)$, $(\gamma - \delta)$ and Y , excluding at most one factor of ± 2 , then Z is not prime.

Proof. By the LCFT

$$\eta(\gamma^p) + \theta(\delta^p) = \frac{1}{2}[(\eta + \theta)(\gamma + \delta)X + (\eta - \theta)(\gamma - \delta)Y].$$

Hence under these conditions, for the expression to be prime, there are two distinct factors on the right hand side, one of which must be ± 2 . ■

We cannot modify these conditions by just reducing two prime factors down to *one*, because taking $p = 1$, $\eta = 5$, $\theta = -6$, $\gamma = 15$ and $\delta = 12$, then $Z = 3$ is prime, but we construct a proof of this modification under the further constraint $\eta \neq \theta \neq 0 \in \mathbf{N}$.

We mention related results. When the expression

$$\gamma^2 + \delta^2 = \frac{1}{2}[(\gamma + \delta)(\gamma + \delta) + (\gamma - \delta)(\gamma - \delta)]$$

is prime, then $\gamma - \delta$ does not share any prime factor with $\gamma + \delta$. ■

Any integer may be represented by $\pm Z$ (put, say, $\delta = 1$. We allow here $Z = 0$). ■

Let $\eta \neq \theta \neq 0$ and $\gamma \neq \delta \neq 0$ be natural numbers and p , X , Y and Z be as in the previous theorem. If the product of $(\gamma - \delta)$, $(\eta - \theta)$ and Y has a prime factor in common with the product $(\gamma + \delta)$, $(\eta + \theta)$ and X , excluding at most one factor of ± 2 for the pairings of $(\gamma - \delta)$ with $(\gamma + \delta)$ or $(\eta - \theta)$ with $(\eta + \theta)$, then Z is not prime.

Sketch of proof. If A and B have a prime common factor, we write $jA = kB$, where the common factor is $(A/k) = (B/j)$. We allocate j and k as positive where possible.

Let p be odd. Define $2W = Y - X$. We will need the following identities.

$$(\gamma + \delta)X = \gamma^p + \delta^p$$

and

$$\gamma X + (\gamma - \delta)W = \gamma^p,$$

$$\delta X + (\delta - \gamma)W = \delta^p.$$

We immediately mention that for pairings of $(\gamma - \delta)$ with $(\gamma + \delta)$, for $p = 3$, $\eta = 1$, $\theta = 2$, $\gamma = 3$ and $\delta = 1$, that $Z = 29$ is prime, so the exclusion of at most one factor of ± 2 is necessary. The same goes for the pairing of $(\eta - \theta)$ with $(\eta + \theta)$, for $p = 1$, $\eta = 3$, $\theta = 1$, $\gamma = 1$ and $\delta = 2$, when $Z = 5$ is prime. But if such pairings occur simultaneously, so both η and θ are either odd or even, and likewise γ and δ , then Z is even $\neq 2$.

Let $j(\gamma - \delta) = k(\gamma + \delta)$ and choose arbitrarily $\gamma > \delta$. Then

$$Z = \frac{1}{2}((\gamma - \delta)/k)[\eta((j + k)X + 2kW) + \theta((j - k)X - 2kW)].$$

For Z to factorise in the way specified, we need to ensure the θ term cannot be negative, so that the term in [] is not 1 or 2. The θ term is

$$\theta((j-k)X - 2kW) = \theta\{(j-k)[\Sigma(s=0, (p-1)/2)[((j+k)/(j-k))^{p-1-2s}]] - (j+k)[\Sigma(s=0, (p-3)/2)[((j+k)/(j-k))^{p-2-2s}]]\}\delta^{p-1}.$$

This equates to $\theta(j-k)(\delta^{p-1})$, so for $(\gamma - \delta)/k > 2$, Z is not prime.

If $j(\gamma - \delta) = k(\eta + \theta)$, then choosing j and k positive, that is, $(\gamma - \delta)/k > 1$, we have

$$Z = (\gamma - \delta)[(j/k)\delta^p + \eta(X + 2W)],$$

so Z factorises.

With $j(\gamma - \delta) = kX$ under scrutiny, we obtain

$$Z = (\gamma - \delta)[\eta((j/k)\gamma + W) + \theta((j/k)\delta - W)].$$

Suppose the term in [] was 1, then we would have $(j/k)\delta < W$, so we would deduce

$$X\delta < (\gamma - \delta)W = X\delta - \delta^p,$$

which is impossible, hence Z is not prime.

If $j(\eta - \theta) = k(\gamma + \delta)$, then

$$Z = (\eta - \theta)[(j/k)\theta X + \gamma^p],$$

and Z factorises, because $(\eta - \theta)/k > 1$.

If $j(\eta - \theta) = k(\eta + \theta)$, then choosing arbitrarily $\eta > \theta$,

$$Z = \frac{1}{2}(\eta - \theta)[((j/k) + 1)\gamma^p + ((j/k) - 1)\delta^p]$$

so since $j/k > 1$ and in *this* instance we specify $(\eta - \theta)/k > 2$, Z again factorises.

For the case $j(\eta - \theta) = kX$, allocating $\eta > \theta$, the value of Z is

$$Z = (\eta - \theta)[(j/k)(\gamma + \delta)\theta + \gamma^p].$$

Since $(\eta - \theta)/k > 1$, Z factorises.

Suppose $jX = kY$. Then

$$Z = \frac{1}{2}X[\eta((\gamma + \delta) + (\gamma - \delta)(j/k)) + \theta((\gamma + \delta) - (\gamma - \delta)(j/k))].$$

We can choose arbitrarily $\gamma > \delta$. To ensure the term in [] is not 1 or 2, we need to evaluate the θ term. Now

$$j/k = 1 + \{2(\delta\gamma^p - \gamma\delta^p)/((\gamma - \delta)(\gamma^p - \delta^p))\},$$

so the θ term is the positive value

$$\theta((\gamma + \delta) - (\gamma - \delta)(j/k)) = 2\theta\delta^p(\gamma + \delta)/(\gamma^p - \delta^p).$$

If X/k is even, so are γ and δ . For X/k odd, the $k[]$ term is even. So Z is not prime.

Now consider $j(\gamma + \delta) = kY$, which gives

$$Z = (\gamma + \delta)[(\eta\gamma + \theta\delta)(j/k) - W].$$

So combining the facts

$$(\eta\gamma + \theta\delta) > \gamma + \delta$$

and

$$Y - W \geq Y - 2W = X,$$

we verify that the term in [] is positive and > 1 , implying that Z factorises.

Lastly, for $j(\eta + \theta) = kY$, we evaluate that

$$Z = (\eta + \theta)[\gamma Y - W(\gamma + \delta) + \theta(\gamma - \delta)(j/k)]$$

so that

$Z = (\eta + \theta)[\gamma X + W(\gamma - \delta) + \theta(\gamma - \delta)(j/k)],$
and choosing arbitrarily $\gamma > \delta$ gives Z is not prime. ■

The same theorem carries over for η and θ integers, with two prime factors instead of one, because the terms in [] can now be ± 1 or ± 2 . ■

No representations of primes are of the form

$$\gamma^p - \delta^p,$$

except for the possibilities $p = 1$, or $\delta = (\gamma - 1)$ and p prime.

Proof. If $\alpha - \beta = \gamma \uparrow (p^m) - \delta \uparrow (p^m)$ is prime, with $\alpha, \beta, \gamma, \delta, \varepsilon, \mu \in \mathbf{N}$ from now on, then the second FSFT gives $m = 1$ (otherwise (*) above factorises), and

$$\alpha - \beta = [\alpha^{1/p} - \beta^{1/p}] \{ \Sigma(s = 0, p - 1) [\alpha^{s/p}] [\beta^{(p-1-s)/p}] \}$$

is prime, the derivation of which implies α and β are powers of p , i.e.

$$\alpha = \gamma^p, \beta = \delta^p,$$

and either

$$\gamma - \delta = 1$$

or

$$\Sigma(s = 0, p - 1) [\gamma^s] [\delta^{p-1-s}] = 1,$$

the latter corresponding to $p = 1$, so we choose the former.

If p is not prime, say $p = jq$, then because

$$\gamma = \alpha^{1/p} = \alpha^{1/qj} = (\alpha^{1/q}) \uparrow (1/j)$$

is a natural number, so is $\alpha^{1/q}$, and similarly for $\beta^{1/q}$. Then the prime $\alpha - \beta$ can be represented by the product

$$(***) \quad [\alpha^{1/q} - \beta^{1/q}] \{ \Sigma(s = 0, q - 1) [\alpha^{s/q}] [\beta^{(q-1-s)/q}] \}.$$

Now if $a > 1$ and $x > y$, we obtain the inequality

$$(x - y)^a = (x - y)^{a-1} (x - y) < x^{a-1} (x - y) < x^a - y^a.$$

Inserting $x = \alpha^{1/p}$, $y = \beta^{1/p}$ and $a = p/q$ has the consequence

$$1 = [\alpha^{1/p} - \beta^{1/p}] = [\alpha^{1/p} - \beta^{1/p}] \uparrow (p/q) < [\alpha^{1/q} - \beta^{1/q}].$$

Thus in (***) the first and second terms $\neq 1$, and all terms involve sums of natural numbers – a contradiction. Hence p is prime. ■

2.4 Divisibility theorems.

Under the conditions of the previous theorem, p divides

$$\gamma^p - \delta^p - 1.$$

Proof. By Fermat's theorem, if p is any prime and γ and δ are integers, then p divides $(\gamma^p - \gamma)$ and $(\delta^p - \delta)$, so p divides $(\gamma^p - \delta^p - \gamma + \delta) = (\gamma^p - \delta^p - 1)$. ■

Let $p > 2$ be even, $\gamma > \delta \geq 1$ and $\gamma - \delta \neq 1$, then

$$\gamma^p - \delta^p$$

has at least three factors.

Proof. Consider $\gamma \uparrow p - \delta \uparrow p$. This may, for even p , be factorised as
 $(\gamma - \delta)(\gamma^{p-1} + \gamma^{p-2}\delta + \gamma^{p-3}\delta^2 + \dots + \delta^{p-1})$

or as

$$(\gamma + \delta)(\gamma^{p-1} - \gamma^{p-2}\delta + \gamma^{p-3}\delta^2 - \dots - \delta^{p-1}).$$

Since $\gamma - \delta \neq \gamma + \delta$, if there are only two factors, which is the minimum if $\gamma - \delta \neq 1$, then

$$\gamma - \delta = (\gamma^{p-1} - \gamma^{p-2}\delta + \gamma^{p-3}\delta^2 - \dots - \delta^{p-1})$$

and

$$\gamma + \delta = (\gamma^{p-1} + \gamma^{p-2}\delta + \gamma^{p-3}\delta^2 + \dots + \delta^{p-1}),$$

so adding these gives successively

$$\gamma = \gamma^{p-1} + \gamma^{p-3}\delta^2 + \dots + \gamma\delta^{p-2}$$

and

$$\gamma \geq \gamma^{p-1} + \gamma^{p-3} + \dots + \gamma,$$

which is impossible. ■

We cannot dispense with the condition $\gamma - \delta \neq 1$, because if $\gamma = 2$, $\delta = 1$ and $p = 4$, then $\gamma^p - \delta^p = 15$. A more general theorem follows next.

Let $p = (2 \uparrow k_0) \prod_{i=1}^n (q_i \uparrow k_i)$, where the q_i are distinct odd primes, and $\gamma > \delta \geq 1$. Then $\gamma^p - \delta^p$ has at least $\sum_{i=0}^n k_i$ factors, and at least $1 + \sum_{i=0}^n k_i$ factors when $\gamma - \delta \neq 1$.

Proof. Let $q_0 = 2$. For the first pass through, consider all factors of $p = \prod_{i=0}^n (q_i \uparrow k_i)$ except for one unexponentiated factor q_r . This product is just $x_r = \prod_{i=0}^n \prod_{j=0}^{k_i-1} (q_i^j)$, omit r for one i (q_i). Then $p = (x_r)(q_r)$. By the equation at the end of section 2.2

$$\gamma^p - \delta^p = [(\gamma \uparrow x_r) - (\delta \uparrow x_r)][\sum_{s=0}^{q_r-1} [\gamma \uparrow x_r s][\delta \uparrow x_r (q_r - 1 - s)]].$$

We now have at least two factors. We can then expand out $(\gamma \uparrow x_r) - (\delta \uparrow x_r)$ recursively, using the same formula, yielding at least one extra factor each time.

We continue iteratively, until we end up with $\gamma - \delta$, which can be a proper factor or the trivial factor 1, which we ignore. We have now $\sum_{i=0}^n k_i$ iterations, giving at least $\sum_{i=0}^n k_i$ factors if $\gamma - \delta = 1$ or at least $1 + \sum_{i=0}^n k_i$ factors otherwise. ■

Let $p = (2 \uparrow k_0)t$, where $t = \prod_{i=1}^n (q_i \uparrow k_i)$, the q_i are distinct odd primes, and arrange $\gamma > \delta \geq 1$. Then $\gamma \uparrow p + \delta \uparrow p$ has at least $1 + \sum_{i=1}^n k_i$ factors.

Proof. t is odd, and may be represented in a similar manner as before as $t = (y_r)(q_r)$. By another formula at the end of chapter 1, section 4

$$\varepsilon^t + \mu^t = [(\varepsilon \uparrow y_r) + (\mu \uparrow y_r)][\sum_{s=0}^{q_r-1} [\varepsilon \uparrow y_r s][(-\mu) \uparrow y_r (q_r - 1 - s)]].$$

Put $\varepsilon = \gamma \uparrow (2 \uparrow k_0)$ and $\mu = \delta \uparrow (2 \uparrow k_0)$. The number of factors is obtained by recursion as previously, where, if prime, the final factor $\varepsilon + \mu$ will not add to the result. ■

If $p \neq 1$, $\chi_1 = (\delta \uparrow p) + (\varepsilon \uparrow p)$ is prime

and $\chi_2 = (\varepsilon \uparrow p) - (\mu \uparrow p)$ is prime

then $\chi_1 - \chi_2$ is not prime unless $\chi_1 = 5$ and $\chi_2 = 3$.

Proof. $\chi_1 - \chi_2 = (\delta \uparrow p) + (\mu \uparrow p)$ is even $\neq 2$ or $= 2$, otherwise $\chi_1 = 2$ or $\chi_2 = 2$. Now both $p = 2^t$ and p is prime, so $p = 2$. If $\chi_1 - \chi_2 = 2$, then $\delta = \mu = 1$, so $(\varepsilon - 1) = 1$, $\varepsilon = 2$ and $\chi_1 = 5$ and $\chi_2 = 3$. If $\chi_1 = 2$ then $\delta = \varepsilon = 1$ and $\chi_2 = 1 - \mu^2$, which is impossible. So $\chi_2 = 2 = (\varepsilon - \mu)(\varepsilon + \mu)$, and if $(\varepsilon - \mu) = 1$ then $2 = 2\mu + 1$, which is impossible. Hence $\chi_1 - \chi_2$ is not prime or $\chi_1 = 5$ and $\chi_2 = 3$. ■

If $p \neq 1$, $\chi_3 = (\delta \uparrow p) + (\varepsilon \uparrow p)$ is prime
and $\chi_4 = (\varepsilon \uparrow p) + (\mu \uparrow p)$ is prime
then $\chi_3 - \chi_4$ is not prime unless $\chi_3 = 5$ and $\chi_4 = 2$.

Proof. This results from the previous theorem. Alternatively, assume $\chi_3 - \chi_4$ is prime. We prove a partial contradiction. Then $\chi_3 - \chi_4 = (\delta \uparrow p) - (\mu \uparrow p)$, so both $p = 2^t$ and p is prime, so $p = 2$ and $(\delta - \mu) = 1$. Suppose $\chi_3 \neq 2$ and $\chi_4 \neq 2$, then for $\chi_3 - \chi_4$ to be prime it must $= 2$. Hence $2 = \delta^2 - (\delta - 1)^2 = 2\delta - 1$, which is impossible. Hence we have primes $\chi_3 = \delta^2 + \varepsilon^2 \neq 2$ and $\chi_4 = (\delta - 1)^2 + \varepsilon^2 = 2$, so $\varepsilon = 1$, $\delta = 2$ and $\chi_3 = 2^2 + 1 = 5$. ■

2.5 Fermat's little theorem.

We note that *the binomial expansion of $\gamma^p - \delta^p$ for $\gamma = (\delta + 1)$ is*
$$\sum_{r=1}^p \binom{p}{r} [\delta^{p-r}] \delta^{p-r}.$$

That p divides $(\delta + 1)^p - \delta^p - 1$ is easy to prove directly by a binomial expansion, the expression being

$$p\delta^{p-1} + [p(p-1)/2]\delta^{p-2} + \dots + p\delta,$$

so if p is prime the factorial denominators do not divide p . ■

We extend the above result. *For p prime, p divides*

$$(\delta + 1)^p - (\delta - x)^p - x - 1.$$

Proof. For two adjacent numbers, p divides

$$(\delta + 1)^p - \delta^p - 1 \text{ and } \delta^p - (\delta - 1)^p - 1.$$

Hence p divides their sum. The result follows by induction. ■

Corollary. *If p is prime, then p divides*

$$y^p - (y - x)^p - w$$

if and only if

$$x \equiv w \pmod{p}.$$

Putting $y = x$, this gives Fermat's little theorem, $y^p - y \equiv 0 \pmod{p}$, from the binomial theorem. ■

With $z = y - x$, we find that *if $y \not\equiv z \pmod{p}$ then*

$$\sum_{r=1}^p \binom{p}{r} [y^{p-r} z^{r-1}] \equiv 1 \pmod{p}. \quad \blacksquare$$

If $y^p - y$ is divisible by p , then so is

$$y^{n(p-1)+1} - y.$$

Proof. Since $y^{2p-1} - y^p = y^{p-1}(y^p - y)$ is divisible by p , the sum $(y^{2p-1} - y^p) + (y^p - y)$ is also, with the general result following by recursion. The proof extends to divisibility by any natural number m instead of a prime p . ■

Examples. Putting $p = 3$, we have for any odd natural number q

$$y^q - y \equiv 0 \pmod{6},$$

and putting $p = 5$, so $q = 4n + 1$, or $p = 7$, giving $q = 6n + 1$, etc. implies

$$y^q - y \equiv 0 \pmod{6p}. \blacksquare$$

Expressions with Bernoulli numbers B^k inside quotation marks will be written as a sum of terms, each of which is a power of B times some number. The powers of B are then interpreted as Bernoulli numbers.

Thus Faulhaber's formula becomes

$$1^{k-1} + 2^{k-1} + \dots + m^{k-1} = [“(m + B)^k - B^k”]/k,$$

and summing the Fermat little theorem terms

$$(1^p - 1) + (2^p - 2) + \dots + (y^p - y)$$

entails the following expression is divisible by p :

$$\{[“(y + B)^{p+1} - B^{p+1}”]/(p + 1)\} - \frac{1}{2}y(y + 1). \blacksquare$$

If we carry out the derivation for Fermat's little theorem again, this time explicitly, we find the general identity for any not necessarily prime q

$$y^q - y = q \sum_{r=1}^{q-1} \{[(q-1)!/(r!(q-r)!)] [“(y + B - 1)^{q-r+1} - B^{q-r+1}”]/(q-r+1)\}. \blacksquare$$

A related use of the binomial theorem is, for $n > 1$ and p prime $> n - 2$, the expression

$$y^p - (y - p)^p + \sum_{k=1, n-2}^p (-1)^k [p!/(k!(p-k)!)] p^k y^{p-k} \equiv 0 \pmod{p \uparrow n}. \blacksquare$$

Let p be odd > 5 . The following expressions are divisible by p , also $p - 2$, if prime.

$$(\delta + 1)^p - \delta^p - 1 - p\delta[\delta^{p-2} + [(p-1)/2]\delta(\delta^{p-4} + 1) + 1],$$

$$(\delta + 1)^p - (\delta - 1)^p - p\delta^2[p - 1 + 2\delta^{p-3}] - 2$$

and

$$(\delta + 1)^p - 2\delta^p + (\delta - 1)^p - p\delta[(p-1)\delta^{p-3} + 2].$$

Proof. The first expression is derived from a binomial expansion of $(\delta + 1)^p$, with the first three and last three terms subtracted. Considering factorial denominators, it is divisible by p or $p - 2$ when either of these are prime, or both when both are prime.

The second and third expressions are obtained from the first under the transformation $\delta \rightarrow -\delta$, respectively adding or subtracting this result from the first. ■

Let n be even and p be odd, with $p > 2n + 1$. Then the following expressions are divisible by all primes between $(p - n)$ and p inclusive:

$$(\delta + 1)^p - \sum_{r=0, n}^p \{p!/[r!(p-r)!]\} \delta^r (\delta^{p-2r} + 1),$$

$$(\delta + 1)^p - (\delta - 1)^p - 2 \{ \sum_{r=0, n/2}^p [p!/(2r!(p-2r)!)] \delta^{2r} + \sum_{r=1, n/2}^p [p!/(2r-1)!(p-2r+1)!] \delta^{p-2r+1} \}$$

and

$$(\delta + 1)^p + (\delta - 1)^p - 2\{\sum(r = 0, n/2)[p!/[(2r)!(p - 2r)!]]\delta^{p-2r} + \sum(r = 1, n/2)[p!/[(2r - 1)!(p - 2r + 1)!]]\delta^{2r-1}\}.$$

Proof. By the binomial theorem, the first expression is equal to

$$\sum(s = n + 1, (p + 1)/2)[p!/[(s!(p - s)!)]]\delta^s(\delta^{p-2s} + 1).$$

To determine the summation range, there are $p + 1$ terms in the expansion of $(\delta + 1)^p$, and we are subtracting $2(n + 1)$ terms, so the number remaining is $p - 2n - 1$. The upper range in the summation is $(p - 2n - 1)/2 + n + 1 = (p + 1)/2$.

To show $p > 2n + 1$, for there to be no cancellations with primes, the lowest factor term of the largest $p!/(p - s)!$ is $(p - n)$, and if prime this must be greater than the concurrent greatest divisor term of $p!/(p - s)!$ by $s = n + 1$.

Thus no factorial denominators divide primes in the numerator between $(p - n)$ and p .

Under the transformation $\delta \rightarrow -\delta$, we obtain

$$-(\delta - 1)^p - \{\sum(r = 0, n/2)[p!/[(2r)!(p - 2r)!]]\delta^{2r}(1 - \delta^{p-4r}) + \sum(r = 1, n/2)[p!/[(2r - 1)!(p - 2r + 1)!]]\delta^{2r-1}(1 - \delta^{p-4r+2})\}$$

is divisible by all primes between $(p - n)$ and p inclusive.

Hence by adding this expression with the corresponding expression for $+\delta$, or by subtracting it, we obtain the two subsequent divisibility results. ■

We investigate analogues of Fermat's little theorem for primes between $(p - n)$ and p .

Let n be even and p be odd, with $p > 2n + 1$. Then the following expressions are divisible by all primes between $(p - n)$ and p inclusive:

$$(\delta + 1)^p - (\delta - x)^p - x - 1 - \sum(r = 1, n)[p!/[(r!(p - r)!)]\{["[(\delta + B)^{p-r+1} - (\delta - x - 1 + B)^{p-r+1}"]/(p - r + 1)] + ["[(\delta + B)^{r+1} - (\delta - x - 1 + B)^{r+1}"]/(r + 1)]\},$$

$$(\delta + 1)^p - (\delta - 1)^p - (\delta - x)^p + (\delta + x)^p - 2x - 2 - 2\sum(r = 1, n/2)\{[p!/[(2r)!(p - 2r)!]]["[(\delta + B)^{2r+1} - (\delta - x - 1 + B)^{2r+1}"]/(2r + 1)] + [1/[(2r - 1)!(p - 2r + 1)!]]["[(\delta + B)^{p-2r+2} - (\delta - x - 1 + B)^{p-2r+2}"]/(p - 2r + 2)]\}$$

and

$$(\delta + 1)^p + (\delta - 1)^p - (\delta - x)^p - (\delta + x)^p - 2\sum(r = 1, n/2)\{[p!/[(2r)!(p - 2r)!]]["[(\delta + B)^{p-2r+1} - (\delta - x - 1 + B)^{p-2r+1}"]/(p - 2r + 1)] + [1/[(2r - 1)!(p - 2r + 1)!]]["[(\delta + B)^{2r} - (\delta - x - 1 + B)^{2r}"]/2r]\}.$$

Proof. We use Faulhaber's formula, noting

$$\sum(s = 0, x)(\delta - s)^q = \sum(s = 0, \delta)s^q - \sum(s = 0, \delta - x - 1)s^q. \blacksquare$$

Put $y = \delta + 1 = x + 1$. Then by direct transcription *the following expressions are divisible by all primes between $(p - n)$ and p , for n even, p odd and $p > 2n + 1$:*

$$y^p - y - \sum_{(r=1, n)} [p!/[r!(p-r)!]] \\ \{ [“(y+B-1)^{p-r+1} - (B-1)^{p-r+1}”]/(p-r+1) \\ + [“(y+B-1)^{r+1} - (B-1)^{r+1}”]/(r+1) \},$$

$$y^p - (y-2)^p + 2(y-1)^p - 2y \\ - 2 [\sum_{(r=1, n/2)} \{ [p!/[(2r!)(p-2r)!] \\ [“(y+B-1)^{2r+1} - (B-1)^{2r+1}”]/(2r+1) \\ + [1/[(2r-1)!(p-2r+1)!] \\ [“(y+B-1)^{p-2r+2} - (B-1)^{p-2r+2}”]/(p-2r+2) \}]]$$

and

$$y^p + (y-2)^p - 2(y-1)^p \\ - 2 [\sum_{(r=1, n/2)} \{ [p!/[(2r!)(p-2r)!] \\ [“(y+B-1)^{p-2r+1} - (B-1)^{p-2r+1}”]/(p-2r+1) \\ + [1/[(2r-1)!(p-2r+1)!] \\ [“(y+B-1)^{2r} - (B-1)^{2r}”]/2r \} \}]. \blacksquare$$

We now consider polynomial forms. *If*

$$x_i \equiv y_i \pmod{n} \text{ and } r_i \equiv s_i \pmod{n}$$

then

$$\sum r_i [x_i \uparrow t_i] \equiv \sum s_i [y_i \uparrow t_i] \pmod{n}.$$

If n is prime and

$$t_i = K_i n + u_i,$$

then by Fermat's little theorem

$$\sum r_i [x_i \uparrow t_i] \equiv \sum s_i [y_i \uparrow (K_i + u_i)] \pmod{n}. \blacksquare$$

For $m, p > 0, n, q > 1 \in \mathbf{N}$, there is an isomorphism between additive $k \pmod{n}$ and, for fixed q , multiplicative $q \uparrow k$, so for $k = p^m$, by the second FSFT example of section 4 with $f = 1$, we obtain

$$q \uparrow (p^m) \equiv 1 \pmod{(q-1)}.$$

Consequently

$$q \uparrow (\sum (p_i \uparrow m_i)) \equiv 1 \pmod{(q-1)},$$

so for any $u_i > 0 \in \mathbf{N}$ we derive the implication

$$\sum (t = 1, u_i) (p_i \uparrow m_i) = u_i (p_i \uparrow m_i), \\ q \uparrow (\sum u_i (p_i \uparrow m_i)) \equiv 1 \pmod{(q-1)}.$$

By the FAFT, we also obtain the following results for p odd:

$$q \uparrow (p^m) \equiv -1 \pmod{(q+1)}$$

and

$$q \uparrow (\sum (i = 1, j) (p_i \uparrow m_i)) \equiv (-1)^j \pmod{(q+1)},$$

which indicates a corresponding equation extending to p_i even (put $p_i = 1, u_i = v_i \uparrow m_i$)

$$q \uparrow (\sum u_i (p_i \uparrow m_i)) \equiv (-1)^{\uparrow} (\sum u_i p_i) \pmod{(q+1)}. \blacksquare$$

2.6 The occupancy theorem.

For p odd prime *quadratic reciprocity* theorems follow from Fermat's little theorem by considering $y(y^{(p-1)/2} - 1)(y^{(p-1)/2} + 1) \equiv y((y^2)^{(p-1)/2} - 1) \equiv 0 \pmod{p}$, so all squares $\neq 0 \pmod{p}$ belong to the $(y^{(p-1)/2} - 1)$ equivalence class [31].

Both $y^{(p-1)/2} \equiv 1$ and $y^{(p-1)/2} \equiv -1 \pmod{p}$ have $(p-1)/2$ root positions. For squares, we assert (the *occupancy theorem*, proved next) that these are all occupied by specific numbers, so there is an isomorphism between complex roots $y^{(p-1)/2} = 1$ at one extremity and non-empty equivalence classes of $y^2 \pmod{p}$ with $y^{(p-1)/2} \equiv 1 \pmod{p}$ at the other. ■

We now prove the occupancy theorem, also applicable on adding γp to all ranges.

Assigning all numbers \pmod{p} , p prime, $m^2 \neq n^2$ if and only if $m \neq n$ and $m \neq (p-n)$.

Proof. A two way implication holds. We will prove that $m^2 - n^2 \equiv 0 \pmod{p}$ leads to a contradiction, which would mean $(m-n)(m+n) = vp$ for some v .

Put $m > n$ and $m, n \leq (p-1)/2$, so $(m+n) < p-1$ and also $(m-n) < (p-1)/2$. But p , being prime, must be a factor of $(m-n)$, $(m+n)$ or both, and this is impossible.

If $p > m \neq n > (p-1)/2$, then

$$2p-1 > (m+n) > p \text{ and } (p-3)/2 \geq (m-n) \geq 1,$$

so neither $(m+n)$ nor $(m-n)$ is divisible by p

If say $n < (p-1)/2$ and $p > m \geq (p-1)/2$ then the only possibility is $(m+n) = p$, since

$$(m-n)(m+n) = [\text{a number} < p][\text{a number} \geq (p-1)/2]. \blacksquare$$

The little theorem is more generally written as $yu(y^{(p-1)/2} - u^{(p-1)/2})(y^{(p-1)/2} + u^{(p-1)/2})$, for which *the LCFT implies*

$$u(y^p) - y(u^p) = (y^2 - u^2)W = (y^2 - u^2)\Sigma(r=0, (p-3)/2)[y^{2r+1}u^{p-2r-2}] \equiv 0 \pmod{p},$$

so that W factorises. ■

For p odd prime, quadratic reciprocity theorems give a factorisation of the Fermat expression $y^{n(p-1)+1} - y$, by considering $y(y^{n(p-1)/2} - 1)(y^{n(p-1)/2} + 1)$. ■

Our alternative formulation of the expression is

$$yu\{[y^{n(p-1)/2}] - [u^{n(p-1)/2}]\}\{[y^{n(p-1)/2}] + [u^{n(p-1)/2}]\},$$

so this time *the LCFT implies*

$$\begin{aligned} u(y^{n(p-1)+1}) - y(u^{n(p-1)+1}) &= (y^2 - u^2)W \\ &= (y^2 - u^2)\Sigma(r=0, (n(p-1)/2) - 1)[y^{2r+1}u^{n(p-1)-2r-1}] \equiv 0 \pmod{p}, \end{aligned}$$

and W again factorises further. ■

Note also the variation that *for p prime and $j > 0$*

$$0 \pmod{p} \equiv [(y \uparrow p) - y] \uparrow [p \uparrow (j-1)],$$

and since intermediate terms in the binomial expansion are $\equiv 0 \pmod{p}$

$$\begin{aligned} 0 \pmod{p} &\equiv [y \uparrow (p \uparrow j)] + \{(-y) \uparrow [p \uparrow (j-1)]\} \\ &\equiv y\{y \uparrow [(p \uparrow j) - 1] + (-1) \uparrow j\}. \end{aligned}$$

We derive the result when p is an odd prime that if j is odd

$$0 \pmod{p} \equiv y\{y \uparrow \{[(p \uparrow j) - 1]/2\} - 1\}\{y \uparrow \{[(p \uparrow j) - 1]/2\} + 1\},$$

and if j is even

$$-2y \pmod{p} \equiv \text{the same expression.}$$

If $y \neq 0 \pmod{p}$ in the latter, $-2 \pmod{p}$ uniquely factorises as either

$$(-1)(2) \pmod{p}$$

so

$$0, 1, 3 \text{ or } -2 \pmod{p} \equiv y^{\uparrow\{[(p \uparrow j) - 1]/2\}}$$

or as

$$(1)(-2) \pmod{p}$$

so

$$0, 2, -1 \text{ or } -3 \pmod{p} \equiv y^{\uparrow\{[(p \uparrow j) - 1]/2\}}. \blacksquare$$

The above technique can be used in the context of solving an n th degree polynomial equation with Heegner integer coefficients and at least $(n - 4)$ such integer solutions.

Note that $y \equiv 0 \pmod{p}$ and $y \equiv 1 \pmod{p}$ are always present, the latter as a square \pmod{p} . The following theorem is useful in determining some further $\equiv \pm 1 \pmod{p}$ interrelationships between various $y^{(p-1)/2}$.

Let $0 < y < p$, with p odd (for example p prime) and $m \in \mathbf{N}$, then

$$y^{(p-1)/2} \equiv (-1)^{(p-1)/2} (mp - y)^{(p-1)/2} \pmod{p}.$$

Proof. First, consider $(p - 1)/2$ even. A binomial expansion of the right hand side, leaving out terms in mp to a power, which are $\equiv 0 \pmod{p}$, indicates that $y^{(p-1)/2} \equiv (-y)^{(p-1)/2} \pmod{p}$.

If $(p - 1)/2$ is odd, then the binomial expansion gives $y^{(p-1)/2} \equiv -(-y)^{(p-1)/2} \pmod{p}$. ■

Our theorem has the following consequences.

Taking the typical example for the $p = 11$ table below, y^5 repeats mod 11 in three regions, **A**, **B** and **C**, the above equation representing symmetries in regions **B** and **C**.

Table: $p = 11$, $(p - 1)/2 = 5$.

$y \equiv \pmod{p}$	y^5	$y^5 \pmod{11}$	region
0	0	0	A
1	1	1	B $0 < n \leq (p - 1)/2$
2	32	-1	
3	243	1	
4	1024	1	
5	3125	1	
6	7776	-1	C $(p - 1)/2 < n < p$
7	16807	-1	
8	32768	-1	
9	59049	1	
10	100000	-1	
$11 \equiv 0 \pmod{11}$			repeats

For $(p - 1)/2$ odd, if $0 < n \leq (p - 1)/2$, i.e. region **B**, then there are k terms $\equiv 1 \pmod{p}$ and $(p - 1)/2 - k$ terms $\equiv -1 \pmod{p}$, so there must be in the $(p - 1)/2 < n < p$ region **C**, k terms $\equiv -1 \pmod{p}$ and $(p - 1)/2 - k$ terms $\equiv +1 \pmod{p}$, giving the complete set of $(p - 1)/2$ root positions for both $1 \pmod{p}$ and $-1 \pmod{p}$.

Table: $p = 17$, $(p - 1)/2 = 8$.

$y \equiv (\text{mod } p)$	y^8	$y^8 \pmod{17}$	region
0	0	0	A
1	1	1	B $0 < n \leq (p - 1)/2$
2	256	1	
3	6561	-1	
4	65536	1	
5	390625	-1	
6	1679616	-1	
7	5764801	-1	
8	16777216	1	
9	43046721	1	C $(p - 1)/2 < n < p$
10	100000000	-1	
11	214358881	-1	
12	429981696	-1	
13	815730721	1	
14	1475789056	-1	
15	2562890625	1	
16	4294967296	1	
$17 \equiv 0 \pmod{17}$			repeats

If $(p - 1)/2$ is *even*, with the k terms $\equiv 1 \pmod{p}$ for region **B** below, there are k terms $\equiv 1 \pmod{p}$ in region **C**, opposite in sign to the odd case. Thus there are $2k$ slots for $2k = (p - 1)/2$ quadratic residues of 1^2 to $4k^2$ in the combined **B** and **C** region, and these slots in **B** (and **C**) are completely occupied. So $k = (p - 1)/4$ in the **B** region, and similarly the residues $\equiv -1 \pmod{p}$ occupy k slots in this region, likewise in region **C**. ■

Note the generalised Fermat little theorem with $q = (p - 1)/2$ prime gives a formula for $y^{(p-1)/2} \pmod{p}$.

We now prove the *occupancy theorem*.

If $m \neq n \leq (p - 1)/2$, with p prime, then $m^2 \neq n^2 \pmod{p}$.

Proof. We will prove that $m^2 - n^2 \equiv 0 \pmod{p}$ leads to a contradiction, which would mean $(m - n)(m + n) = kp$ for some k .

Say $m > n$, then $n < (p - 1)/2$, so $m + n < p - 1 < p$ and likewise $(m - n) < p - 1$. But p , being prime, must be a factor of $(m - n)$, $(m + n)$ or both, and this is impossible. ■

Since 1 is a square, it follows from the above considerations that *when* $(p - 1)/2$ *is even*, $(-1)^{(p-1)/2} \equiv 1 \pmod{p}$, *and when* $(p - 1)/2$ *is odd*, $(-1)^{(p-1)/2} \equiv -1 \pmod{p}$. ■

We have dealt with recurrence relations between numbers of the form $y^{(p-1)/2} \pmod{p}$. Another useful relation to determine the value of $y^{(p-1)/2} \pmod{p}$ is

$$(uv)^{(p-1)/2} \pmod{p} \equiv [u^{(p-1)/2} \pmod{p}][v^{(p-1)/2} \pmod{p}]. \blacksquare$$

A *basic question* is then: *when is a prime a square* \pmod{p} ?

If we look at the table for squares, say in the (mod 7) example that follows, there are p squares from 0 to $p^2 - 1 \pmod{p^2}$, being $0^2, 1^2, \dots, (p-1)^2$.

Table: $p = 7$, squares (underlined) to $p^2 = 49$. Region **E** columns = region **F** columns.

region D	<u>0</u>
region E	<u>1</u> 2 3 <u>4</u> 5 6 7 8 <u>9</u>
region F	10 11 12 13 14 15 <u>16</u> 17 18 19 20 21 22 23 24 <u>25</u> 26 27 28 29 30 31 32 33 34 35 <u>36</u> 37 38 39 40 41 42 43 44 45 46 47 48
next p^2	<u>49</u>

Since, by the binomial theorem for squares,

$$(p + n)^2 \equiv n^2 \pmod{p},$$

these p squares fill, in p iterations (mod p), all the squares that are possible (mod p^2).

Likewise, since

$$(p - n)^2 \equiv n^2 \pmod{p},$$

those squares which are non-zero (mod p^2), repeat in just two non-overlapping sets (mod p^2), regions **E** and **F**.

Although the non-constructive ‘pigeon hole principle’ can act as a barrier to understanding, we now apply this principle here.

We have previously proved that there are $(p - 1)/2$ non-zero squares (mod p). The first overlapping set $\neq 0$, in region **E**, being the first $(p - 1)/2$ squares (mod p^2), maps to precisely $(p - 1)/2$ separate squares (mod p), because otherwise there would be less than $(p - 1)/2$ of them. We are using here full occupancy of the square slots. ■

A ‘crossing out’ method can be used, analogous to the ‘sieve of Eratosthenes’ for primes, for determining whether a number is or is not a square (mod p). Set up a grid of width p and depth $> (p - 1)^2/4p$ and $< [(p - 1)^2/4p] + 1$ with the first column labelled 0. Determine the column for a number n given by $n \pmod{p}$. Put an X in column 0, an X in column 1 with no space between columns 0 and 1, an X in column 4 with two spaces between columns 1 and 4, and so on, increasing the number of spaces by two each time and continuing into other rows if necessary. If the column corresponding to n is reached, it is a square (mod p), otherwise it is not. ■

2.7 Reciprocity.

Quadratic reciprocity is often introduced through binary quadratic forms, discussed in a later work, where we will prove the following ‘supplementary’ law:

$$2^{(p-1)/2} \equiv 1 \pmod{p} \text{ if } p \equiv \pm 1 \pmod{8},$$

$$2^{(p-1)/2} \equiv -1 \pmod{p} \text{ if } p \equiv \pm 3 \pmod{8}$$

and quadratic reciprocity itself, which states, *for p and q distinct odd primes* [10]

$$[p^{(q-1)/2} \pmod{q}][q^{(p-1)/2} \pmod{p}] \equiv (-1)^{(p-1)(q-1)/4}.$$

If we recast this as

$$[p^{(q-1)/2} \pmod{q}] \equiv [(-1)^{(q-1)/2} q^{(p-1)/2} \pmod{p}],$$

the theorem is seen to be equivalent to the form in which Gauss put it

Let p and q be distinct odd primes. If $q \equiv 1 \pmod{4}$, i.e. $(q-1)/2$ is even, then p is a square \pmod{q} if and only if q is a square \pmod{p} . If $q \equiv 3 \pmod{4}$, i.e. $(q-1)/2$ is odd, then p is a square \pmod{q} if and only if -q is a square \pmod{p} . ■

We note in the table below that if a prime $p \pmod{12} \equiv 1$ or $-1 \pmod{p}$ then $3^{(p-1)/2} \equiv 1 \pmod{p}$, and if $p \pmod{12} \equiv 5$ or $-5 \pmod{p}$ then $3^{(p-1)/2} \equiv -1 \pmod{p}$.

Table: p prime, q = 3.

$3^{(p-1)/2} \equiv \pm 1 \pmod{p}$	$p \pmod{12}$
$9 \equiv -1 \pmod{5}$	5
$27 \equiv -1 \pmod{7}$	-5
$243 \equiv 1 \pmod{11}$	-1
$729 \equiv 1 \pmod{13}$	1
$6561 \equiv -1 \pmod{17}$	5
$19683 \equiv -1 \pmod{19}$	-5
$177147 \equiv 1 \pmod{23}$	-1
$4782969 \equiv -1 \pmod{29}$	5
$14348907 \equiv -1 \pmod{31}$	-5

This is part of a more general result, supplementary to quadratic reciprocity, relating a prime $p \pmod{4q}$ to $q^{(p-1)/2} \pmod{p}$.

We can evaluate all $(p-1)/2$ non-zero squares \pmod{p} by the method already given.

Quadratic reciprocity then gives, for a given prime $q < p$ that is such a square, there is a bijection between $q^{(p-1)/2} \pmod{p}$ and $\pm p^{(q-1)/2} \pmod{q}$, the latter of which depends on \pmod{q} , and for which a square or non-square p depends on $\pmod{4}$.

Thus, $q = 0$ maps to $p = 0 \pmod{4q}$. If the $\pmod{4q}$ region does not contain 0, non-zero squares determined by $q^{(p-1)/2} \equiv 1 \pmod{p}$ are equivalent to half of the $4q$ values of $p \neq 0 \pmod{4q}$, and non-squares map to the remaining $2q$ values $\pmod{4q}$. ■

For p prime, if $y^t \equiv 1 \pmod{p}$, then for any $s \in \mathbf{N}$, since $y^{s(p-1)} \equiv 1 \pmod{p}$, there exists an $r = 1/s \pmod{p}$ such that

$$y^{(p-1)/r} \equiv 1 \pmod{p}.$$

If y is prime, r must divide $(p-1)$, so likewise if y is composite. ■

For $0 < n < p$, (for example with p prime), $m \in \mathbf{N}$ and r a divisor of $(p-1)$, then

$$y^{(p-1)/r} \equiv (-1)^{(p-1)/r} (mp - y)^{(p-1)/r} \pmod{p}.$$

Proof. The result parallels the argument of the previous theorem where we had $r = 2$, by using $(p - 1)/r$ instead of $(p - 1)/2$. ■

We now ask: *when is a number an r th power (mod p), with r a divisor of $(p - 1)$?*

Table: $p = 7$ and $r = 3$, cubes (underlined) to $p^3 = 343$.

region I	<u>0</u>					
region J	6	<u>1</u>	2	3	4	5
	7	<u>8</u>	9	10	11	12
	13					
	14	15	16	17	18	19
	20					
	21	22	23	24	25	26
	<u>27</u>					
region K	...					
	63	<u>64</u>	65	66	67	68
	69					
	...					
	119	120	121	122	123	124
	<u>125</u>					
	...					
210	211	212	213	214	215	
<u>216</u>						
next p^3	<u>343</u>					

There are p r th powers from 0 to $p^r - 1 \pmod{p^{\uparrow r}}$, being $0^r, 1^r, \dots, (p - 1)^r$.

Once again, by the binomial theorem,

$$(p + n)^r \equiv n^r \pmod{p},$$

these p r th powers fill, in r iterations (mod p), all the r th powers that are possible (mod $p^{\uparrow r}$).

For r *even*, where effectively we are dealing with a certain type of square,

$$(p - n)^r \equiv n^r \pmod{p},$$

so those r th powers which are non-zero (mod $p^{\uparrow r}$) repeat in just two non-overlapping sets (mod $p^{\uparrow r}$), regions **J** and **K**. But for r *odd*

$$(p - n)^r \equiv -n^r \pmod{p},$$

yields no new information this way, although we are able to assert that for $(p - 1)/r = 2$ as above, the $(y^{(p-1)/2} \pm 1) \pmod{p}$ equivalence classes for squares and non-squares are equivalently partitioned as $(y^{r(p-1)/2r} \pm 1) \pmod{p}$. Thus in this case y^r belongs to the $((y^r)^{(p-1)/2r} \pm 1) \pmod{p}$ equivalence classes, i.e. $y^r \equiv \pm 1 \pmod{p}$. For $(p - 1)/r = k$, the y^r belong to the $(y^r)^k \equiv 1 \pmod{p}$ equivalence classes. ■

Masser's ABC conjecture states that if $\gamma(n)$ is the largest squarefree divisor of n , then for each fixed $\varepsilon > 0$ there are at most finitely many coprime positive integer triples a, b, c with

$$a + b = c, \gamma(abc) < c^{1-\varepsilon}.$$

A special case that has been proved is the Fermat-Catalan conjecture, which asserts that if x , y and z are coprime and $1/p + 1/q + 1/r < 2$ then there are finitely many $x^p + y^q = z^r$.

The absence of solutions for x, y, z coprime when $p, q, r > 2$ is conjectured. ■

2.8 Remarks on Fermat's last theorem.

We make some minor remarks about Fermat's Last Theorem.

If $x^p + y^p = z^p$ where x, y, z and $n < p$ are positive $\in \mathbf{N}$, then $x^{p-n} + y^{p-n} > z^{p-n}$.

Proof. $z > x$, so $z^n > x^n$ and $z^n x^{p-n} > x^p$, with similar statements for y instead of x . Thus $z^n x^{p-n} + z^n y^{p-n} > z^n z^{p-n}$. ■

Corollary. If $x^p + y^p = z^p$, then $x + y - z$ is positive. ■

Let p and q be prime, with $q < p$ and

$$x^p + y^p = z^p$$

as before. Then

$$x^{p-q+1} + y^{p-q+1} - z^{p-q+1} = 6q\mathbb{I}_q$$

(or $= q\mathbb{I}_q$ for $q = 2$ and $= 2q\mathbb{I}_q$ for $q = 3$) for some natural number \mathbb{I}_q .

Proof. By Fermat's little theorem, write $x^q - x = 6q\mathbb{I}\mathbb{I}_x$, $y^q - y = 6q\mathbb{I}\mathbb{I}_y$ and $z^q - z = 6q\mathbb{I}\mathbb{I}_z$ (where instead, for $q = 2$, $x^q - x = q\mathbb{I}\mathbb{I}_x$, etc. and for $q = 3$, $x^q - x = 2q\mathbb{I}\mathbb{I}_x$, etc.). Here $\mathbb{I}\mathbb{I}_x$, $\mathbb{I}\mathbb{I}_y$ and $\mathbb{I}\mathbb{I}_z$ are given by the 'explicit' Bernoulli formulae. Then

$$\begin{aligned} 0 &= x^{p-q}(6q\mathbb{I}\mathbb{I}_x + x) + y^{p-q}(6q\mathbb{I}\mathbb{I}_y + y) - z^{p-q}(6q\mathbb{I}\mathbb{I}_z + z) \\ &= -6q\mathbb{I}_q + (x^{p-q+1} + y^{p-q+1} - z^{p-q+1}). \quad \blacksquare \end{aligned}$$

Corollary. The conditions of the above converse to Fermat's Last Theorem imply

$$x^{p-1} + y^{p-1} - z^{p-1} = 2\mathbb{I}_2,$$

$$x^{p-2} + y^{p-2} - z^{p-2} = 6\mathbb{I}_3,$$

...

$$x + y - z = 6p\mathbb{I}_p. \quad \blacksquare$$

The following formula was used by Euler in proving Fermat's last theorem for $n = 3$:

$$(na^2 + b^2)(t^2 + nu^2) = n(at + bu)^2 + (nau - bt)^2.$$

The formula used in the proof of Lagrange's theorem that every natural number may be represented by a sum of four squares is related to quaternionic multiplication where

$$e^{\uparrow}(i\theta + jp + k\sigma) = (\cos\theta + isin\theta)(\cos p + jsin p)(\cos\sigma + ksin\sigma).$$

We can take the point of view that the exponential addition is non-abelian and the theorem can be extended to a formula similar to Euler's above:

$$\begin{aligned} (na^2 + b^2 + c^2 + d^2)(t^2 + nu^2 + nv^2 + nw^2) &= \\ n(at + bu + cv + dw)^2 + (nau - bt + ncw - ndv)^2 &+ \\ + (nav - ct + ndu - nbw)^2 + (naw - dt + nbv - ncu)^2. &\blacksquare \end{aligned}$$