Numbers Equal to the Sum of Two Square Numbers

Laurent Théry
INRIA Sophia Antipolis

Abstract

This note presents a formalisation of an elementary proof of the fact that a number n can be written as the sum of two square numbers if and only if each prime factor p of n that is equal to 3 modulo 4 has its exponent in the decomposition of n that is even.

1 Definitions and Notations

In order to present the proof of this theorem, we first need to introduce some predicates:

- **Divisibility**: n divides m, written $n|m$, if there exists a number q such that $m = nq$.

- **Primality**: p is prime, written $prime(p)$, if p has *exactly* two positive divisors 1 and p.

- **CoPrimality**: p and q are co-prime, written $coprime(p, q)$, if 1 is their unique common positive divisor.

- **Modulo**: p is equal to q modulo n, written $p \equiv q\,[n]$, if n divides $p - q$.

and some functions:

- **Factorial**: $p!$ is defined as $\prod_{i=1}^{p} i$.

- **Gcd**: the greatest common divisor of two numbers p and q is written $p \,\hat{}\, q$.

- **Quotient**: the integer quotient of the division of p by q is written p/q.
- **Remainder**: the remainder of the division of p by q is written $p \,\%\, q$.

2 Basic Theorems

Theorem 2.1 (Gauss) *if $m|np$ and $coprime(m, n)$ then $m|p$.*

This theorem does not belong to our development, nevertheless we outline its proof. The key point of the proof is that divisibility is compatible with the substraction: if $m|n$ and $m|p$ then $m|n-p$. Now, we have the hypothesis $m|np$ and we also have that $m|mp$. Remembering Euclid's algorithm and using the compatibility of the substraction we can derive that $m|(m \hat{} n)p$. As we have $coprime(m, n)$, we get the expected result $m|p$.

Theorem 2.2 (Bezout) *let m and n two integers, then there exist u and v such that $mu + nv = m \hat{} n$.*

Once again the proof of this theorem follows Euclid's algorithm to compute the gcd of m and n.

3 Cancellation theorem

Theorem 3.1 (Cancellation) *If $ab \equiv ac\,[m]$ and $coprime(a, m)$ then $b \equiv c\,[m]$.*

We have $m|ab - ac$. This means $m|a(b - c)$. Applying Theorem 2.1, we get that $m|b - c$, i.e. $b \equiv c\,[m]$.

4 Fermat's Little theorem

Theorem 4.1 (Fermat) *If $prime(p)$ and $coprime(a, p)$ then $a^{p-1} \equiv 1\,[p]$.*

First of all, because $prime(p)$, we have $coprime(p, (p - 1)!)$. Using Theorem 3.1, it is sufficient to prove that $a^{p-1}(p-1)! \equiv (p-1)!\,[p]$. We have $a^{p-1}(p-1)! = (\prod_{i=1}^{p-1} a)(\prod_{i=1}^{p-1} i) = \prod_{i=1}^{p-1}(ia)$. Using the properties of the modulo, we get that $a^{p-1}(p-1)! \equiv \prod_{i=1}^{p-1}((ia) \,\%\, p)\,[p]$. Now using again Theorem 3.1, we know that $ia \equiv ja\,[p]$ implies that $i \equiv j\,[p]$. So we have $\prod_{i=1}^{p-1}((ia) \,\%\, p) = (p-1)!$ since the first product contains exactly $p - 1$ distinct and non null numbers smaller than p.

5 Wilson's theorem

Theorem 5.1 (Coprime inverse) *If $prime(p)$ and $coprime(p, n)$, then there exists m such that $mn \equiv 1\,[p]$ with $1 \le b \le p-1$ and $coprime(p, m)$.*

From Theorem 2.2, we know that there exist u and v such that $up + vn = 1$. This means that $vn \equiv 1\,[p]$. It is then sufficient to take $m = v \,\%\, p$.

Theorem 5.2 (Wilson) *If $prime(p)$ then $(p-1)! \equiv -1\,[p]$.*

We first consider the case where $p = 2$. In that case, we $(p-1)! = 1! = 1$ and $-1 \equiv 1\,[2]$. Now if $p > 2$, we have $(p-1)! = (\prod_{i=2}^{p-2} i)(p-1)$. We are left with proving $\prod_{i=2}^{p-2} i \equiv 1\,[p]$. By Theorem 5.1, we know that there exists j such that $1 \le j \le p-1$ and $ij \equiv 1\,[p]$. Note that $j \ne i$ otherwise $i+1$ would be a divisor of p. Furthermore since $1 < i < p-1$ we also need to have $1 < j < p-1$. This means that in the product $\prod_{i=2}^{p-2} i$ for each i there is also its inverse modulo p. So $\prod_{i=2}^{p-2} i \equiv 1\,[p]$.

Theorem 5.3 (Wilson converse) *If $(p-1)! \equiv -1\,[p]$ and $p > 1$ then $prime(p)$.*

We prove this by contradiction. Suppose that p is composite, i.e. $p = qr$ with $1 < q < p$ and $1 < r < p$. If $q \ne r$, then $p | \prod_{i=1}^{p-1} i$ so $(p-1)! \equiv 0\,[p]$. If $q = r$, we have $p = q^2$. If $p = 4$, then $(p-1)! = 6$, so $(p-1)! \equiv 2\,[4]$. If $p > 4$, we have that $2 < q$ so $2q < q^2 = p$. As we have $0 < q < 2q < p$, we have $2q^2 | \prod_{i=1}^{p-1} i$. This means that $(p-1)! \equiv 0\,[p]$.

6 Main theorems

Theorem 6.1 (square root of -1) *If $prime(p)$ and $\neg(p|b)$ and $p|(a^2+b^2)$, then there exists i such that $i^2 \equiv -1\,[p]$.*

Since $prime(p)$, we have $coprime(p, b)$, so by Theorem 5.1, there exists u such that $ub \equiv 1\,[p]$. Let's take $i = au$. To prove that $i^2 \equiv -1\,[p]$, it is enough to prove that $i^2b^2 \equiv -b^2\,[p]$ by Theorem 3.1 since $coprime(p, b^2)$. $i^2b^2 = (au)^2b^2 = a^2(ub)^2$. So $i^2b^2 \equiv a^2\,[p]$. Since $a^2 \equiv -b^2\,[p]$ the conclusion follows.

Theorem 6.2 (square root of -1 corollary) *If $prime(p)$ and $p = a^2+b^2$, then there exists i such that $i^2 \equiv -1\,[p]$.*

We apply Theorem 6.1 since $p|(a^2+b^2)$ and $prime(p)$ implies $\neg(p|b)$.

Theorem 6.3 (square root of -1 converse) *If $prime(p)$ and there exists i such that $i^2 \equiv -1\,[p]$, then there exist a and b such that $p = a^2 + b^2$.*

Consider k the integer square root of p. We have $k^2 < p < (k+1)^2$ since p is prime. The set $\{x + iy \mid 0 \leq x \leq k \textit{ and } 0 \leq y \leq k\}$ contains $(k+1)^2$ elements. As $p < (k+1)^2$, there exists at least two distinct pairs (x_1, y_1) and (x_2, y_2) such that $x_1 + iy_1 \equiv x_2 + iy_2\,[p]$. We have $x_1 - x_2 \equiv i(y_2 - y_1)\,[p]$. Squaring both sides we get $(x_1 - x_2)^2 \equiv -(y_2 - y_1)^2\,[p]$ Let's take $a = |x_1 - x_2|$ and $b = |y_1 - y_2|$, so we have $a^2 + b^2 \equiv 0\,[p]$. But as we have $0 \leq x_1 \leq k$ and $0 \leq x_2 \leq k$, we deduce that $a^2 \leq k^2 < p$. As the same holds for b we get $b^2 < p$. So $a^2 + b^2 < 2p$. Furthermore as the pairs are distinct, we have $0 < a^2 + b^2$. Altogether we get that the only way $a^2 + b^2 \equiv 0\,[p]$ can be true is that $p = a^2 + b^2$.

Theorem 6.4 (uniqueness) *If $prime(p)$ and then there exist a and b such that $p = a^2 + b^2$, then this pair is unique.*

Suppose that $a^2+b^2 = p = c^2+d^2$. We have $(ad+bc)(ab-bd) = a^2d^2-b^2c^2 = a^2d^2 + b^2d^2 - b^2d^2 + b^2c^2 = (a^2 + b^2)d^2 - (d^2 + c^2)b^2 = pd^2 - pb^2 = p(d^2 - b^2)$. This means that $(ad + bc)(ab - bd) \equiv 0\,[p]$. Since p is prime, a consequence of Theorem 2.1 is that $p|ab - bd$ or $p|ad + bc$. Since $0 < a^2 < p$, $0 < b^2 < p0 < c^2 < p$ and $0 < d^2 < p$, we have $ab - bc = 0$ or $ad + bc = p$.

If $ab = bc$, we have that $a|bc$ but as $coprime(a, b)$ (otherwise p would not be prime), by Theorem 2.1 we get that $a|c$. This means that there exists k such that $c = ka$. We have $ad = bc = bka$, so $d = kb$. So $p^2 = c^2 + d^2 = (ka)^2 + (kb)^2 = k^2(a^2 + b^2)$. This implies that $k = 1$, so $c = a$ and $d = b$.

If $ad + bc = p$, we have $p^2 = (a^2 + b^2)(c^2 + d^2) = (ad + bc)^2 + (ac - bd)^2 = p^2 + (ac - bd)^2$. This means that $ac = bd$. Similarly to the first case, we get $a = d$ and $b = c$.

Theorem 6.5 (square 2) *If $p = 2$ then there exists i such that $i^2 \equiv -1\,[p]$,*

Let's take $i = 1$. We have $i^2 = 1 = (2 - 1)$.

Theorem 6.6 (square 1 modulo 4) *If $prime(p)$ and $p \equiv 1\,[4]$ then there exists i such that $i^2 \equiv -1\,[p]$.*

Let's take $i = ((p-1)/2)!$. Since $p-1$ is even, the division is exact. We have $(p-1)! = \prod_{j=1}^{p-1} j = (\prod_{j=1}^{(p-1)/2} j)(\prod_{j=(p-1)/2+1}^{p-1} j) = i \prod_{j=1}^{(p-1)/2} p - j$. We have $\prod_{j=1}^{(p-1)/2} p - j \equiv \prod_{i=1}^{(p-1)/2} -j \,[p]$. Furthermore $\prod_{j=1}^{(p-1)/2} -j = (-1)^{(p-1)/2} i = i$ since $(p-1)/2$ is even. So we have $(p-1)! \equiv i^2 \,[p]$. By Theorem 5.2 we finally get $i^2 \equiv -1 \,[p]$.

Theorem 6.7 (not square 3 modulo 4) *If $prime(p)$ and $p \equiv 3 \,[4]$ then there is no i such that $i^2 \equiv -1 \,[p]$.*

We do the proof by contradiction. We suppose that there exists i such that $i^2 \equiv -1 \,[p]$. Theorem 6.3 gives us that there exist a and b such that $p = a^2 + b^2$. We do the proof by case analysis.

- If $a \equiv 0 \,[2]$ and $b \equiv 0 \,[2]$, we have $p \equiv 0 \,[4]$.
- If $a \equiv 0 \,[2]$ and $b \equiv 1 \,[2]$, we have $p \equiv 1 \,[4]$.
- If $a \equiv 1 \,[2]$ and $b \equiv 0 \,[2]$, we have $p \equiv 1 \,[4]$.
- If $a \equiv 1 \,[2]$ and $b \equiv 1 \,[2]$, we have $p \equiv 2 \,[4]$.

Each case contradicts $p \equiv 3 \,[4]$.

Theorem 6.8 (div 3 modulo 4) *If $prime(p)$ and $p \equiv 3 \,[4]$ and $p | a^2 + b^2$ then $p | a$.*

The proof is done by contradiction. Suppose that $p | a$, the Theorem 6.1 gives us there exists i such that $i^2 \equiv -1 \,[p]$ but this contradicts Theorem 6.7.

Theorem 6.9 (div square 3 modulo 4) *If $prime(p)$ and $p \equiv 3 \,[4]$ and $p | a^2 + b^2$ then $p^2 | a^2 + b^2$.*

Theorem 6.8 with $a^2 + b^2$ and $b^2 + a^2$ gives us that $p | a$ and $p | b$. It follows that $p^2 | a^2 + b^2$.

Theorem 6.10 (Comp Product) *If there exist a and b such that $m = a^2 + b^2$ and there exist c and d such that $n = c^2 + d^2$, then there exist e and f such that $mn = e^2 + f^2$.*

It is sufficient to take $e = ad + bc$ and $f = ac - bd$.

Theorem 6.11 (Main theorem) *If for all p, $prime(p)$, $p|n$ and $p \equiv 3\,[4]$, there exists α such that, $p^{2\alpha}|n$ and $\neg(p^{2\alpha+1}|n)$, then there exist a and b such that $n = a^2 + b^2$.*

This proof is done by strong induction on n. The base case is the case where n is prime. If $n \equiv 3\,[4]$, Theorem 6.9 would give that $n^2|n$ which is impossible so we have either $n = 2$ or $n \equiv 1\,[4]$. In both case, Theorem 6.5 and Theorem 6.6 gives us an i, such $i^2 \equiv -1\,[p]$. From Theorem 6.3 it follows that there exist a and b such that $n = a^2 + b^2$.

For the inductive case, we consider $p|n$. If we have either $p = 2$ or $p \equiv 1\,[4]$, as we did for the base case, it is easy to show that there exist a and b such that $p = a^2 + b^2$. Using the inductive hypothesis, we also have that there exist c and d such that $p/n = c^2 + d^2$. Theorem 6.10 lets us conclude. Now if we have $p \equiv 3\,[4]$, we know that there exists α such that $p^{2\alpha}|n$. As we have $p^{2\alpha} = (p^\alpha)^2 + 0^2$ and applying the inductive hypothesis there exists a and b such that $n/p^{2\alpha} = a^2 + b^2$, Theorem 6.10 lets us conclude.

Theorem 6.12 (Main theorem converse) *If there exist a and b such that $n = a^2 + b^2$, then for all p, $prime(p)$, $p|n$ and $p \equiv 3\,[4]$, there exists α such that $p^{2\alpha}|n$ and $\neg(p^{2\alpha+1}|n)$.*

The proof is done by strong induction on n. If n is prime and $n \equiv 3\,[4]$, Theorem 6.9 gives us that $n^2|n$ which is impossible.

For the inductive case, if $prime(p)$, $p|n$ and $p \equiv 3\,[4]$, Theorem 6.9 and Theorem 6.8 give that $p|a$, $p|b$ and $p^2|a^2+b^2$. Applying the inductive hypothesis on $n/p^2 = (a/p)^2+(b/p)^2$, we get β such that $p^{2\beta}|n/p^2$ and $\neg(p^{2\beta+1}|n/p^2)$. It is then sufficient to take $\alpha = \beta + 1$.