Some Elementary Properties of Prime Numbers

Numbers are fascinating. The natural numbers $\{1, 2, 3, \dots\}$ are the fertile ground in which all our notions of "a number" have taken root. And of all the natural numbers, the prime numbers – defined simply as those natural numbers which cannot be evenly divided by any smaller natural number, except unity – have received more attention from more mathematicians than any other sub-class of the integers.

The purpose of this little paper is to prove four simple propositions about the prime numbers. The first two may be proved quite easily. The last two require much more effort.

1. The odd primes comprise two classes: $\{4m + 1\}$ and $\{4m - 1\}$.
2. No prime p of the form $4m - 1$ can be the sum of two squares.
3. Every prime p of the form $4m + 1$ is the sum of two squares.
4. The representation of p in (3) is unique.

---

1. The odd primes comprise two classes: $\{4m + 1\}$ and $\{4m - 1\}$.

Indeed, the sequence $\{1, 2, 3, 4 * 1 + 0, 4 * 1 + 1, 4 * 1 + 2, 4 * 1 + 3, 4 * 2 + 0, \dots\}$ constitutes the entire set of natural numbers. Consequently, every even number $2, 4, 6, \dots$ is either of the form $4k$ or $4k + 2$, and every odd number is either of the form $4k + 1$ or $4k + 3$. But

$$4k + 3 = 4(k + 1) - 1 = 4m - 1 \quad \text{where} \quad m = k + 1 \quad \bigstar \tag{1}$$

2. No prime p of the form $4m - 1$ can be the sum of two squares.

We use a simple parity argument. $4m - 1$ is an odd number for every $m \in \mathbb{Z}$. Since the square of every even number is even, and the square of every odd number is odd, a sum of two squares $k^2 + l^2$ can only be an odd number if one of k or l is even and the other is odd, because the sum of two odd numbers – or the sum of two even numbers – is always an even number. Suppose that $k = 2i$ is even, and $l = 2j + 1$ is odd. Then

$$k^2 + l^2 = (2i)^2 + (2j + 1)^2 = 4i^2 + 4j^2 + 4j + 1 = 4(i^2 + j^2 + j) + 1 \tag{2}$$

from which we conclude that the sum $k^2 + l^2$ must be of the form $4m + 1$, and not of the form $4m - 1$. $\bigstar$

3. Every prime p of the form $4m + 1$ is the sum of two squares.

Because this proposition is harder to prove than the first two (and also because we will need to utilize some notation that may not be as familiar as $+, -, \times, \div$, and $=$), I will define a few number-theoretic concepts and some useful symbols, then outline the procedure we will follow before demonstrating the third proposition.

The greatest common divisor (gcd for short) of two or more distinct integers: Given two distinct integers (k, l), we define their greatest common divisor d to be the largest natural number that divides both k and l evenly. In symbols, $\gcd(k, l) = d$. Similarly, given a finite set of m different integers $\{n_1, n_2, n_3, \ldots, n_m\}$, we define the $\gcd$ to be the greatest natural number that evenly divides all of the n_i. The Euclidean Algorithm is an efficient tool for finding the greatest common divisor of any two distinct integers.

Modular arithmetic was devised by Carl F. Gauss about two hundred years ago. We say that two integers (k, l) are *congruent modulo m* if the remainder left upon dividing k by m is equal to the remainder left when l is divided by m. This relationship is expressed symbolically as $k \equiv l \pmod{m}$. It should be apparent that

$$k \equiv l \pmod{m} \quad \Longleftrightarrow \quad m \text{ evenly divides the difference } (k - l).$$

Since the only possible remainders when an integer is divided by m are $\{0, 1, 2, \ldots, m-1\}$, we say that the congruence modulo m partitions the integers into m equivalence classes, each one defined by $\{n \equiv r_i \pmod{m}\},\ 0 \le r_i \le m - 1$. It should be apparent that any set of m consecutive integers may be used to define these same m equivalence classes $\pmod{m}$.

Diophantine analysis – named after Diophantus of Alexandria – is the branch of mathematics concerned with finding the integral solutions of algebraic equations. The number of such solutions is often finite, even when the equation is inteterminate. For instance, the equation $a^2 + b^2 = 25$, whose solutions comprise a circle of radius 5 centered on $(0, 0)$ and therefore consist of uncountably many points $(a, b) \in \mathbb{R}^2$, has just twelve integral solutions: $(0, 5), (5, 0), (0, -5), (-5, 0), (3, 4), (4, 3), (3, -4), (4, -3), (-3, 4), (-4, 3), (-3, -4)$, and $(-4, -3)$.

With these preliminaries completed, we are ready to prove proposition 3. The proof will proceed by way of these seven intermediate steps.

A. The Diophantine equation $ax + by = m$ $(a, b, m \in \mathbb{Z})$ has an integral solution $\{x, y\}$ if and only if $\gcd(a, b)$ divides m.

B. The set of residue classes $\pmod{p}$, where p is any prime and excluding zero, form a multiplicative group of order $p - 1$.

C. (A) and (B) imply **Wilson's Theorem**: If p is prime, $(p - 1)! \equiv -1 \pmod{p}$.

D. If a prime p is of the form $4m + 1$, the congruence $x^2 + 1 \equiv 0 \pmod{p}$ has two solutions.

E. We will next prove **Thue's Lemma**: If p is prime and p does not divide a, the congruence $xa \equiv \pm y \pmod{p}$ has a nontrivial integral solution $\{x, y\}$ $\left(|x| < \sqrt{p} \text{ and } |y| < \sqrt{p}\right)$.

F. If the congruence $x^2 + 1 \equiv 0 \pmod{p}$ is solvable (where p is prime), p can be expressed as the sum of two squares.

G. Taken together, (D) and (F) above imply the truth of proposition 3.

3(A). The Diophantine equation $ax + by = m$ $(a, b, m \in \mathbb{Z})$ has an integral solution $\{x, y\}$ if and only if $\gcd(a, b)$ divides m.

The "only if" part is easier, so we'll prove that first. We seek to prove that if the Diophantine equation $ax + by = m$ has an integral solution $\{x, y\}$, then d, the $\gcd(a, b)$, must divide m. But this is obvious. Since d divides a, it must also divide ax (x being integral). By the same token, d divides by. Therefore d divides $ax + by$, which equals m by hypothesis.

It remains to show that if $d = \gcd(a, b)$ divides m, the equation $ax + by = m$ has an integral solution $\{x, y\}$. We will do this by analyzing the steps in the previously mentioned **Euclidean Algorithm**, by means of which the $\gcd(a, b)$ can be calculated.

The Euclidean Algorithm proceeds by a process of successive divisions. We assume without loss of generality that both a and b are positive natural numbers, and that $a > b$. By the elementary properties of division we may write

$$a = b \times q_1 + r_1 \quad \text{where} \quad 0 \le r_1 \le b - 1$$

The Euclidean Algorithm proceeds by iterating this process:

$$\begin{aligned} a &= b \times q_1 + r_1 \\ b &= r_1 \times q_2 + r_2 \\ r_1 &= r_2 \times q_3 + r_3 \\ &\vdots \\ r_{n-2} &= r_{n-1} \times q_n + r_n \\ r_{n-1} &= r_n \times q_{n+1} + 0 \end{aligned} \tag{3}$$

Now it should be apparent that this process must eventually terminate with a remainder $r_{n+1} = 0$, because each remainder is strictly less than the preceding one. It is also apparent that the final non-zero remainder, r_n, is the greatest common divisor of (a, b). Our hypothesis can now be proved by solving for r_n in terms of a and b:

$$\begin{aligned} r_1 &= a - b \times q_1 \\ r_2 &= b - r_1 \times q_2 \\ &= b - (a - bq_1) \times q_2 \\ r_3 &= r_1 - r_2 \times q_3 \\ &= a - bq_1 - (b - ((a - bq_1)q_2) \times q_3 \\ &= a - bq_1 - bq_3 + aq_2q_3 - bq_1q_2q_3 \\ &= a(1 + q_2q_3) - b(q_1 + q_3 + q_1q_2q_3) \\ &\vdots \end{aligned} \tag{4}$$

The series of equations (4) may evidently be continued until we reach an equation for $r_n = d$, the greatest common divisor of (a, b). Therefore we may write $ax + by = d$ with integral coefficients x, y, because all of the q_i are integers. And if d divides m evenly (say $d * n = m$) we have $a(nx) + b(ny) = n(ax + by) = n * d = m$. ★

3(B). The set of residue classes $\pmod{p}$, where p is any prime and excluding zero, form a multiplicative group of order $p-1$.

This may be a bit of overkill, because we don't need to associate all the properties of an algebraic group with the $p-1$ residue classes associated with the integers $\{1, 2, 3, \ldots, p-1\}$ to complete the proof of proposition 3. But it's a simple way to characterize the main property (existence of multiplicative inverses) we do need, and a brief digression into abstract algebra will be fun, besides.

In algebra, a **group** is a set of elements $G = \{g\}$ and an associated binary operation $\circ$ that satisfy the following axioms, or rules.

1. **Closure:** G is closed under $\circ$. If $g, h \in G$, then $g \circ h \in G$.
2. **Associativity:** $g \circ (h \circ j) = (g \circ h) \circ j$ for every $g, h, j \in G$.
3. **Identity:** There is one $I \in G$ such that $I \circ g = g \circ I = g$ for every $g \in G$.
4. **Inverse:** For each $g \in G$, there is a g^{-1} such that $g \circ g^{-1} = g^{-1} \circ g = I$.

We must show that the $p-1$ residue classes $\{n \equiv r_i \pmod{p}\}$ $(1 \le r_i \le p-1)$ satisfy these four rules under ordinary multiplication modulo (p).

Closure: Each of the r_i, $1 \le r_i \le p-1$, is relatively prime to p; or, in other words, none of the r_i has a factor (other than unity) in common with p, which is prime by hypothesis. Therefore no product $r_i \times r_j$ of any two of these numbers can be divisible by p. But this is equivalent to saying that $r_i \times r_j$ must be congruent $\pmod{p}$ to one of the values $\{1, 2, 3, \ldots, p-1\}$. In other words, the specified set of residue classes is closed under multiplication $\pmod{p}$.

Associativity: This follows immediately from the associative property of ordinary multiplication.

Identity: The number 1, the identity element under ordinary multiplication, is clearly an identity element for multiplication $\pmod{p}$, because $1 \times r_i = r_i \times 1 = r_i$ for each of the $p-1$ residue classes.

Inverse: If $a \in \{1, 2, 3, \ldots, p-1\}$, we seek to find $a^{-1} \in \{1, 2, 3, \ldots, p-1\}$ such that $a * a^{-1} \equiv 1 \pmod{p}$. But

$$a * x \equiv 1 \pmod{p} \quad \iff \quad \text{the equation } ax - py = 1 \text{ has an integral solution } \{x, y\}$$

and this latter fact was established in 3(A) above, because $\gcd(a, p) = 1$. This solution x is the inverse element we seek: any x in such a solution cannot be divisible by p; therefore it must fall into one of the $p-1$ residue classes $\{n \equiv r_i \pmod{p}\}$ $(1 \le r_i \le p-1)$. ★

We note in passing that because the non-zero integers taken modulo (p) form a multiplicative group of order $p-1$, we may immediately assert Fermat's Little Theorem:

$$\text{For any prime } p, \text{ if } \gcd(a, p) = 1,\ a^{p-1} \equiv 1 \pmod{p}.$$

3(C). 3(A) and 3(B) imply Wilson's Theorem: If p is prime, $(p-1)! \equiv -1 \pmod{p}$.

This result is almost immediate. The two equivalence classes defined by $r_1 \equiv 1 \pmod{p}$ and $r_{p-1} \equiv -1 \pmod{p}$ are easily seen to be their own reciprocals. The rest of the equivalence classes (for odd p) may be grouped together pairwise as multiplicative inverses, by group property (4), above. Therefore $(p-1)! \equiv 1^{\frac{p-3}{2}} * (1) * (-1) \equiv -1 \pmod{p}$ when p is odd.

In the special case $p = 2$, we observe that $1! = 1 \equiv 1 \equiv -1 \pmod{2}$: this completes the proof that Wilson's Theorem is true for every prime p. ★

3(D). If a prime p is of the form $4m+1$, the congruence $x^2+1 \equiv 0 \pmod{p}$ has two solutions.

We proceed by constructing the two solutions explicitly. We observe first that

$$\begin{gathered}(p-1) \equiv -1\\(p-2) \equiv -2\\(p-3) \equiv -3\\\vdots\\\left(\frac{p+1}{2}\right) \equiv -\left(\frac{p-1}{2}\right)\end{gathered} \tag{5}$$

where all the preceding congruences are taken $\pmod{p}$. Substituting these expressions in $(p-1)! = 1 * 2 * 3 * \cdots * (p-1)$, we see that

$$(p-1)! \equiv (-1)^{\frac{p-1}{2}} \left(1 * 2 * 3 * \cdots * \frac{p-1}{2}\right)^2 \pmod{p} \tag{6}$$

and if we substitute $4m+1$ for p in expression (6) above and combine that with Wilson's Theorem we obtain

$$(p-1)! + 1 \equiv 0 \equiv (-1)^{2m}(1 * 2 * 3 * \cdots * 2m)^2 + 1 \pmod{p} \tag{7}$$

From (7) we conclude that if $p = 4m+1$ is prime, the congruence $x^2+1 \equiv 0 \pmod{p}$ is solvable and has the two roots $\pm(2m)!$ ★

3(E). Prove Thue's Lemma: If p is prime and p does not divide a, the congruence $ax \equiv \pm y \pmod{p}$ has a nontrivial integral solution $\{x, y\}$ ($|x| < \sqrt{p}$ and $|y| < \sqrt{p}$).

The proof depends on the pigeonhole principle, also known as Dirichlet's box principle: if m items are placed in n boxes, and $m > n$, then at least one box must contain more than one item.

Given a prime p, let k be the smallest natural number such that $k^2 > p$. Now $(k-1)^2 < p$, because a prime p cannot be a perfect square. Let us form all the distinct pairs of natural numbers (x, y) that can be created with $0 \leq x, y \leq k-1$. There are evidently k^2 such pairs: $(0,0), (0,1), (1,0), (1,1), \ldots, (k-1, k-1)$. Each such pair (x_i, y_i) can be associated with a remainder r_j via the congruence $ax_i + y_j \equiv r_j \pmod{p}$. But there are k^2 such number pairs, and only p possible values of the remainder r_j, because $0 \leq r_j \leq (p-1)$. Since

$k^2 > p$, at least two of the pairs (x_i, y_i) must be associated with the same remainder r', by the pigeonhole principle.

Let's consider any two solutions (x_m, y_m) and (x_n, y_n) that satisfy $ax + y \equiv r' \pmod{p}$. We may write

$$\begin{aligned} ax_m + y_m &\equiv r' \pmod{p} \\ ax_n + y_n &\equiv r' \pmod{p} \\ a(x_m - x_n) + (y_m - y_n) &\equiv 0 \pmod{p} \\ a(x_m - x_n) &\equiv y_n - y_m \pmod{p} \qquad (8) \end{aligned}$$

We cannot possibly have $y_m = y_n$, because if that were so we should also have $x_m = x_n$ by congruence (8) above (and because p does not divide a by hypothesis). But we chose the (x_i, y_i) in such a way that no number pair was replicated. By the same token, $x_m \neq x_n$. And by the method used to construct the number pairs (x_i, y_i), we must have

$$\begin{aligned} -\sqrt{p} < -(k-1) \leq (x_m - x_n) \leq (k-1) < \sqrt{p} \quad &\text{and also} \\ -\sqrt{p} < -(k-1) \leq (y_m - y_n) \leq (k-1) < \sqrt{p}. & \end{aligned}$$

Therefore $(x, y) = (x_m - x_n, y_n - y_m)$ is the non-trivial solution whose existence was to be demonstrated. ★

3(F). If the congruence $x^2 + 1 \equiv 0 \pmod{p}$ is solvable (where p is prime), p can be expressed as the sum of two squares.

Let us suppose that p is prime, and that a is a root of the congruence $x^2 + 1 \equiv 0 \pmod{p}$. By Thue's Lemma we can find a "small" solution $\{x_a, y_a\}$ to the congruence $ax \equiv \pm y$. So we may write

$$a^2 + 1 \equiv 0 \pmod{p} \quad \longrightarrow \quad a^2x_a^2 + x_a^2 \equiv 0 \pmod{p} \qquad (9a)$$

$$ax_a \equiv \pm y_a \pmod{p} \quad \longrightarrow \quad a^2x_a^2 \equiv y_a^2 \pmod{p} \qquad (9b)$$

Substituting (9b) into (9a) and reordering terms we obtain $x_a^2 + y_a^2 \equiv 0 \pmod{p}$. This can only be true if some integer n exists such that $x_a^2 + y_a^2 = np$. But according to the result obtained in Thue's Lemma, $x_a^2 < p$ and also $y_a^2 < p$. Therefore we may write

$$x_a^2 + y_a^2 < p + p \quad \longrightarrow \quad x_a^2 + y_a^2 < 2p \quad \longrightarrow \quad n < 2$$

and, since the only positive integer less than 2 is unity, $x_a^2 + y_a^2 = p$. ★

3(G). Taken together, 3(D) and 3(F) above imply the truth of proposition 3.

This is patently obvious. By result 3(D) above, if p is of the form $4m + 1$, the congruence $x^2 + 1 \equiv 0 \pmod{p}$ has two integral solutions: $\{\pm(2m)!\}$. And by 3(F), if for some integer $x, x^2 + 1 \equiv 0 \pmod{p}$, then $p = x^2 + y^2, (x, y) \in \mathbb{Z}^2$. ★

The result we have just proved – that if a prime $p = 2m + 1$ for some integer m, then there are integers x, y such that $x^2 + y^2 = p$ – is commonly known as Fermat's Two-Squares Theorem, after Charles de Fermat, who gave the result in a letter to Marine Mersenne dated Christmas Day, 1640. Fermat did not give a proof. The first proof was given by

Leanhard Euler more than a century later, in 1749. Euler was a gifted mathematician who made voluminous contributions to mathematics in both number theory (discrete mathematics) and analysis (aka calculus, or the mathematics of the continuum). The proof of our fourth proposition – that the representation of a prime p as the sum of two squares is unique – was developed by Euler, who used the technique illustrated next as a method for factoring large composite numbers.

4. The representation of a prime p as the sum of two squares is unique.

We shall show that if an integer n can be represented as the sum of two squares in more than one way it is a composite number, and therefore not prime. So let us suppose we are given an odd number n that can be expressed as the sum of two squares in at least two ways: $a^2 + b^2 = c^2 + d^2 = n$. Since n is odd, each of the pairs (a, b) (c, d) must contain one even integer and one odd integer. Assume that a and c are even, so that b and d are odd. Clearly we must have

$$\begin{aligned} a^2 + b^2 &= c^2 + d^2 \\ a^2 - c^2 &= d^2 - b^2 \\ (a-c)(a+c) &= (d-b)(d+b) \qquad (10) \end{aligned}$$

It is clear that all four factors $(a-c), (a+c), (d-b), (d+b)$ in (10) above are even numbers: the first two are the sum and difference of two even integers, and the latter two are the sum and difference of two odd numbers. Next we choose $j = \gcd((a-c), (d-b))$ so that $(a-c) = jl$ and $(d-b) = jm$, with $\gcd(l, m) = 1$. Clearly j is an even number, since both $(a-c)$ and $(a+c)$ are even. Substituting these expressions in equation (10) we see that

$$\begin{aligned} jl(a+c) &= jm(b+d) \\ l(a+c) &= m(b+d) \qquad (11) \end{aligned}$$

Since l and m are relatively prime, we see that m must be a divisor of $(a+c)$. So there is an integer k such that

$$\begin{aligned} l(a+c) = l(km) &= m(d+b) \\ \longrightarrow \quad lk &= (d+b) \qquad (11a) \end{aligned}$$

and from (11a) we conclude that k is a divisor of $(d+b)$. And since both $(a+c)$ and $(d+b)$ are even numbers, k must be even, since not both of l and m can be even – if they were, they would have a factor in common, contradicting the way they were chosen.

Let us now consider the product

$$\left(\left(\tfrac{j}{2}\right)^2 + \left(\tfrac{k}{2}\right)^2\right)(l^2 + m^2).$$

Since j and k are both even numbers, and l, m are integers, this is a product of two natural numbers. But this product is clearly equal to $\frac{1}{4}\left[(jl)^2 + (jm)^2 + (kl)^2 + (km)^2\right]$, where $jl = (a-c)$, $jm = (d-b)$, $kl = (d+b)$, and $km = (a+c)$. Putting all this together we see that

$$\begin{aligned}\left(\left(\frac{j}{2}\right)^2+\left(\frac{k}{2}\right)^2\right)(l^2+m^2) &= \tfrac{1}{4}\left[(km)^2+(jl)^2+(kl)^2+(jm)^2\right]\\ &= \tfrac{1}{4}[(a+c)^2+(a-c)^2+(d+b)^2+(d-b)^2]\\ &= \tfrac{1}{4}[2a^2+2c^2+2d^2+2b^2]\\ &= \tfrac{1}{4}[2(a^2+b^2)+2(c^2+d^2)]=n \qquad (12)\end{aligned}$$

This completes the proof of proposition 4: we have demonstrated that if an odd number n can be represented as a sum of two squares in more than one way, n is composite, and not prime. ★