Congruences are respected by addition, subtraction and multiplication:

$$a \equiv b \pmod{n}$$

and

$$c \equiv d \pmod{n}$$

imply

$$a \pm c \equiv b \pm d \pmod{n}$$

and

$$ac \equiv bd \pmod{n}.$$

But congruences do not respect division, for example,

$$14 \equiv 4 \pmod{10}$$

but

$$14/2 = 7 \not\equiv 2 = 4/2 \pmod{10}.$$

Each $a \in \mathbf{Z}$ is congruent to exactly one of the numbers $0, 1, \ldots, n-1$ modulo n. For example $1000 \equiv 6 \pmod 7$. Also there is $b \in \mathbf{Z}$ with $|b| \leq n/2$ such that $a \equiv b \pmod n$. For example $1000 \equiv -1 \pmod 7$.

As $0^2 = 0$, $1^2 = 1$, $2^2 = 4 \equiv 0 \pmod 4$ and $3^2 = 9 \equiv 1 \pmod 4$ then $x^2 \equiv 0$ or $1 \pmod 4$ for all $x \in \mathbf{Z}$. Similarly $x^2 \equiv 0$, 1 or $4 \pmod 8$ for all $x \in \mathbf{Z}$. These observations are useful when studying sums of squares.

Theorem 1 *There are infinitely many primes p with $p \equiv 3$ (mod 4).*

Proof It suffices to prove that for each n there is such a p with $p > n$. Let $N = 4(n!) - 1$. Then $N \equiv 3$ (mod 4). Each prime factor of N is odd, so each is congruent to 1 or 3 modulo 4. Let $N = p_1 p_2 \cdots p_k$. If **all** the p_i are congruent to 1 modulo 4, then $N = p_1 p_2 \cdots p_k \equiv 1 \times 1 \times \cdots \times 1 \equiv 1$ (mod 4), which is false. Therefore at least one of the p_i, let's call it p, is congruent to 3 modulo 4. If $p \leq n$ then $p \mid n!$ and so $N = 4(n)! - 1 \equiv -1$ (mod p) contradicting $p \mid N$. Hence $p > n$, as required. $\square$

The Euclidean algorithm

The King of Number Theory Algorithms!

Theorem 2 *Given a, $b \in \mathbf{N}$ we can compute $g \in \mathbf{N}$ and r, $s \in \mathbf{Z}$ such that*

- $g \mid a$ *and* $g \mid b$, *and*
- $g = ra + sb$.

This g is the *greatest common divisor* of a and b since if $h \in \mathbf{N}$ is a divisor of both a and b then

$$g = ra + sb \equiv r0 + s0 = 0 \pmod{h}.$$

So $h \mid g$ and so $h \leq g$. We write $g = \gcd(a, b)$.

The algorithm:

set $a_1 = a$, $a_2 = b$ and repeat the following step while $a_{j+1} \nmid a_j$:

find $q_j \in \mathbb{N}$ such that $a_{j+2} = a_j - q_j a_{j+1}$ satisfies $0 < a_{j+2} < a_{j+1}$.

When $a_{j+1} \mid a_j$ then $g = a_{j+1}$.

Example:

Let $a = 37$ and $b = 14$. Then

$$\begin{aligned} a_1 &= 37, \\ a_2 &= 14, \\ a_3 &= 37 - 2 \times 14 = 9, \\ a_4 &= 14 - 1 \times 9 = 5, \\ a_5 &= 9 - 1 \times 5 = 4, \\ a_6 &= 5 - 1 \times 4 = 1 \end{aligned}$$

As $1 \mid 4$, the algorithm terminates and $\gcd(37, 14) = 1$.

Computing r and s

It's easiest to do this as one goes along, finding r_j and s_j such that $a_j = r_j a + s_j b$. In our example:

$$\begin{aligned}
a_1 &= 37 = a = 1a + 0b,\\
a_2 &= 14 = b = 0a + 1b,\\
a_3 &= 9 = a_1 - 2a_2 = a - 2b,\\
a_4 &= 5 = a_2 - a_3 = -a + 3b,\\
a_5 &= 4 = a_3 - a_4 = 2a - 5b,\\
a_6 &= 1 = a_4 - a_5 = -3a + 8b.
\end{aligned}$$

Thus $r = -3$ and $s = 8$. I like to set this out in tabular form:

a_j	r_j	s_j
37	1	0
14	0	1
9	1	-2
5	-1	3
4	2	-5
1	-3	8

Solving linear congruences

I restrict to

$$ax \equiv b \pmod{n} \qquad (*)$$

where $\gcd(a, n) = 1$. Then we can find integers r and s with $ra + sn = 1$; then $ra \equiv 1 \pmod{n}$, Multiplying $(*)$ by r gives

$$rax \equiv rb \pmod{n}$$

but

$$rax \equiv 1x \equiv x \pmod{n}$$

so the solution of $(*)$ is $x \equiv rb \pmod{n}$.

As an example we solve

$$14x \equiv 22 \pmod{37}.$$

We know $1 = 8 \times 14 - 3 \times 37$ so that $8 \times 14 \equiv 1 \pmod{37}$. Therefore

$$x \equiv 8 \times 14x \equiv 8 \times 22 = 176 \equiv 28 \pmod{37}.$$

The Euclidean algorithm has some important theoretical consequences. If p is prime, then if $p \nmid a$ the congruence $ax \equiv 1 \pmod{p}$ is soluble, since $\gcd(a, p)$ must be a factor of p, but it can't be p so it's 1. We call the solution of $ax \equiv 1 \pmod{p}$ the *reciprocal* of a modulo p. We tabulate reciprocals modulo 11:

1	2	3	4	5	6	7	8	9	10
1	6	4	3	9	2	8	7	5	10

Here 1 and 10 are their own reciprocals, but the others "pair off". Hence

$$\begin{aligned} & 10! \\ = \; & 1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 \\ = \; & 1 \times (2 \times 6) \times (3 \times 4) \times (5 \times 9) \times (7 \times 8) \times 10 \\ \equiv \; & 1 \times 1 \times 1 \times 1 \times 1 \times 10 \pmod{11} \\ = \; & 10 \equiv -1 \pmod{11}. \end{aligned}$$

In fact $(p-1)! \equiv -1 \pmod{p}$ for all primes p: this is *Wilson's theorem*.

We can almost prove Wilson's theorem. By pairing off each number with its reciprocal, $(p-1)!$ is congruent to the product of all self-reciprocal (modulo p) numbers between 1 and $p-1$ inclusive. Obviously 1 and $p-1$ are self-reciprocal modulo p. If there aren't any more, Wilson's theorem follows. These self-reciprocal numbers are the solutions of $x^2 \equiv 1 \pmod{p}$. So we need this quadratic congruence to only have the obvious solutions $x \equiv \pm 1 \pmod{p}$.

But we need to be careful. It's crucial that p is a prime: note that $5^2 \equiv 1 \pmod{24}$ but $5 \not\equiv \pm 1 \pmod{24}$. We need the following famous result.

Theorem 3 (Euclid's lemma) *Let a and b be integers and p be a prime. If $p \mid ab$ then either $p \mid a$ or $p \mid b$.*

Proof Assume that $p \mid ab$ and $p \nmid a$. Then $\gcd(a,p) = 1$ and so there is $r \in \mathbf{Z}$ with $ra \equiv 1 \pmod{p}$. Then

$$b = 1b \equiv rab \equiv r0 = 0 \pmod{p}$$

as required. □

This has an immediate corollary:

Theorem 4 *Let p be a prime and $a \in \mathbf{Z}$. If $a^2 \equiv 1$ (mod p) then $a \equiv \pm 1$ (mod p).*

Proof Now $a^2 \equiv 1 \pmod{p}$ means that $p \mid (a^2 - 1)$, that is $p \mid (a-1)(a+1)$. By Euclid's lemma either $p \mid (a-1)$ or $p \mid (a+1)$. Thus $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$. □

This allows us to complete the proof of Wilson's theorem. If p is prime, the only numbers between 1 and $p-1$ inclusive which are self-reciprocal modulo p are 1 and $p-1$. The numbers between 2 and $p-2$ inclusive can be paired off into reciprocal pairs. We get $(p-1)! \equiv 1 \times (1 \times \cdots \times 1) \times (p-1) \equiv -1 \pmod{p}$.

Euclid's lemma can be extended to a product of several factors by a straightforward induction; I omit the details:

Theorem 5 *Let p be prime. Suppose that $p \mid a_1 a_2 \cdots a_r$ where the $a_i \in \mathbf{Z}$. Then $p \mid a_i$ for at least one i.*

I'll state but don't prove a generalization of Theorem 4.

Theorem 6 *Let p be a prime, and let $a_1, \ldots, a_n \in \mathbf{Z}$. Then the congruence*

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1} x + a_n \equiv 0 \pmod{p}$$

has at most n distinct solutions modulo p.

Theorem 7 (Fundamental theorem of arithmetic) *Let* $n \in \mathbf{N}$ *with* $n > 1$*. If*

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

with each p_i *and* q_i *prime and where* $p_1 \leq p_2 \leq \cdots \leq p_r$ *and* $q_1 \leq q_2 \leq \cdots \leq q_s$*, then* $r = s$ *and* $p_i = q_i$ *for all* i*.*

Proof Use strong induction. Suppose that each integer m with $1 < m < n$ has unique prime factorization. Consider n. If n is prime then we must have $r = s = 1$ and $n = p_1 = q_1$.

If n isn't prime and $p_1 = q_1$ set $m = n/p_1 = p_2 \cdots p_r = q_2 \cdots q_s$. Then $1 < m < n$. By the inductive hypothesis $r - 1 = s - 1$, so that $r = s$, and $p_i = q_i$ for $2 \leq i \leq r$. We win!

Otherwise $p_1 \neq q_1$. If $p_1 < q_1$ then as $p_1 \mid n = q_1 \cdots q_s$ then $p_1 \mid q_i$ for some i. But as p_1 and q_i are prime, $p_1 = q_i$. But this is impossible, as $p_1 < q_1 \leq q_i$. Similarly it is impossible for $q_1 < p_1$. This completes the inductive proof. $\square$

Powers modulo a prime

Let's consider an example. Modulo 11,

$$2^2 \equiv 4, \quad 2^3 \equiv 8, \quad 2^4 \equiv 5, \quad 2^5 \equiv 10.$$

$$2^6 \equiv 9, \quad 2^7 \equiv 7, \quad 2^8 \equiv 3, \quad 2^9 \equiv 6,$$

$$2^{10} \equiv 1, \quad 2^{11} \equiv 2, \quad 2^{12} \equiv 4, \ldots$$

and we go round in a cycle of length 10. Again modulo 11

$$3^2 \equiv 9, \quad 3^3 \equiv 5, \quad 3^4 \equiv 4, \quad 3^5 \equiv 1,$$

$$3^6 \equiv 3, \quad 3^7 \equiv 5, \cdots$$

and again we go round in a cycle, this time of length 5. However we find $3^{10} = (3^5)^2 \equiv 1^2 \equiv 1 \pmod{11}$. Indeed for $0 < a < 11$ we find $a^{10} \equiv 1 \pmod{11}$.

Theorem 8 (Fermat's little theorem) *Let p be a prime, and a an integer with $p \nmid a$. Then $a^{p-1} \equiv 1$ (mod p).*

Before giving the proof, we give an example illustrating how the method works. We prove first that $3^{10} \equiv 1 \pmod{11}$. Modulo 11,

$$\begin{aligned} 3^{10} \times 10! &= 3^{10} \times 1 \times 2 \times 3 \times 4 \times 5 \\ &\quad \times 6 \times 7 \times 8 \times 9 \times 10 \\ &= 3 \times 6 \times 9 \times 12 \times 15 \\ &\quad \times 18 \times 21 \times 24 \times 27 \times 30 \\ &\equiv 3 \times 6 \times 9 \times 1 \times 4 \\ &\quad \times 7 \times 10 \times 2 \times 5 \times 8 \\ &= 10!. \end{aligned}$$

By Wilson's theorem $-3^{10} \equiv -1 \pmod{11}$.

The general proof is just the observation that this trick always works.

Proof Note that

$$a^{p-1}(p-1)! = \prod_{t=1}^{p-1}(ta) = a(2a)\cdots((p-1)a)$$

and we claim that the factors $a, 2a, \ldots, (p-1)a$ are congruent modulo p to $1, 2, \ldots, p-1$ in some order. To see this note that if $0 < b < p$ then the congruence $ax \equiv b \pmod{p}$ has a unique solution with $0 \leq x < p$ (as $\gcd(a,p) = 1$), and this solution can't be $x = 0$. Thus

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

By Wilson's theorem,

$$-a^{p-1} \equiv -1 \pmod{p}.$$

□

As a consequence we get:

Fermat primality test Let $n > 1$ be an integer.

(1) Pick a with $1 < a < n$,

(2) compute a^{n-1} modulo n,

(3) if $a^{n-1} \not\equiv 1 \pmod{n}$ then n is certainly NOT PRIME; if $a^{n-1} \equiv 1 \pmod{n}$ then n may (or may not) be prime.

Note it is **surprisingly easy** to compute a^r modulo n. **Don't** compute in succession a^2, a^3, $a^4, \ldots, a^r$ modulo n. Instead use 'repeated squaring' trick: if $r = 2s$ is even, first compute $b \equiv a^s \pmod{n}$ and then use $a^r = a^{2s} \equiv b^2 \pmod{n}$; if $r = 2s + 1$ is odd, first compute $b \equiv a^s \pmod{n}$ and then use $a^r = a^{2s+1} \equiv ab^2 \pmod{n}$.

We do a miniature example: $n = 39$, $a = 2$.
To compute $2^{38} = (2^{19})^2 \pmod{39}$ we first compute $2^{19} \pmod{39}$,
to compute $2^{19} = 2(2^9)^2 \pmod{39}$ we first compute $2^9 \pmod{39}$,
to compute $2^9 = 2(2^4)^2 \pmod{39}$ we first compute $2^4 \pmod{39}$,
to compute $2^4 = (2^2)^2 \pmod{39}$ we first compute $2^2 \pmod{39}$.
Now $2^2 = 4$, $2^4 = 4^2 = 16$, $2^9 = 2 \times 16^2 = 512 \equiv 5 \pmod{39}$, $2^{19} \equiv 2 \times 5^2 = 50 \equiv 11 \pmod{39}$ and $2^{38} \equiv 11^2 = 121 \equiv 4 \pmod{39}$. So 39 isn't prime!

We have already discussed the congruence $x^2 \equiv 1 \pmod{p}$ for p prime. When studying sums of two squares we need to consider the congruence $x^2 \equiv -1 \pmod{p}$ for p prime.

We find that for certain primes $p = 2, 5, 13$ etc., the congruence is soluble, but for $p = 3, 7, 11$ etc., there are no solutions. When there are solutions, an argument similar to that for $x^2 \equiv 1$ shows that there are at most two solutions.

We tabulate the solutions for some small p:

p	x	p	x	p	x
2	1	13	± 5	31	-
3	-	17	± 4	37	± 6
5	± 2	19	-	41	± 9
7	-	23	-	43	-
11	-	29	± 12	47	-

Theorem 9 *Let p be a prime number. The quadratic congruence*

$$x^2 \equiv -1 \pmod{p} \qquad (*)$$

is soluble if and only if either $p = 2$ or $p \equiv 1$ (mod 4).

Proof When $p = 2$, $x = 1$ is a solution. Assume now that p is odd. Thus either $p \equiv 1$ or $p \equiv 3$ (mod 4).

Next suppose that $p \equiv 3$ (mod 4). Write $p = 4k + 3$ where $k \in \mathbf{Z}$. If $x \in \mathbf{Z}$ solves $(*)$ then

$$\begin{aligned} x^{p-1} &= x^{4k+2} = (x^2)^{2k+1} \\ &\equiv (-1)^{2k+1} = -1 \pmod{p} \end{aligned}$$

which contradicts Fermat's little theorem.

Finally suppose that $p \equiv 1$ (mod 4). Write $p = 4k+1$ where $k \in \mathbf{N}$. Let $x = (2k)!$. Then

$$\begin{aligned} x^2 &= (-1)^{2k} 1^2 \times 2^2 \times \cdots \times (2k)^2 \\ &= 1(-1)2(-2) \times \cdots \times (2k)(-2k) \\ &\equiv 1(p-1)2(p-2) \times \cdots \times (2k)(p-2k) \\ &= (p-1)! \equiv -1 \pmod{p} \end{aligned}$$

by Wilson's theorem. □

Solving $x^2 \equiv -1 \pmod{p}$

By the previous proof, we can write $p = 4k + 1$ and compute $x = (2k)!$ modulo p. Alas this is not practical for large p since there is no known shortcut for computing $a!$ modulo n. For example for $p = 53$,

$$\begin{aligned} x &\equiv 26! = 403291461126605635584000000 \\ &\equiv 23 \pmod{53}. \end{aligned}$$

But there is a trick. Pick a at random with $0 < a < p$. Then $x \equiv a^k \pmod{p}$ is a solution of $x^2 \equiv -1 \pmod{p}$ with probability $1/2$. (The other half of the time $x \equiv \pm 1$.) If you are unlucky, pick another a.

For example with $p = 53$ and $a = 2$ then $k = 13$ and $x \equiv 2^{13} \pmod{53}$. Now $2^6 = 64 \equiv 11$, $2^{12} \equiv 11^2 = 121 \equiv 15$ and $x \equiv 2^{13} \equiv 2 \times 15 = 30 \pmod{53}$. Note that $30 \equiv -23 \pmod{53}$.

Sums of squares We define

$$S_2 = \{a^2 + b^2 : a, b \in \mathbf{Z}\}$$

as the set of sums of two squares. Of course as $a^2 + b^2 = (\pm a)^2 + (\pm b)^2$ we don't need to consider negative a and b but it's convenient to allow these and to insist that zero is a squares. Obviously $0 \in S_2$ and no element of S_2 is negative. Our task will be to find which elements of $\mathbf{N}$ lie in S_2.

n	a^2+b^2	n	a^2+b^2	n	a^2+b^2
1	1^2+0^2	7	-	13	3^2+2^2
2	1^2+1^2	8	2^2+2^2	14	-
3	-	9	3^2+0^2	15	-
4	2^2+0^2	10	3^2+1^2	16	4^2+0^2
5	2^2+1^2	11	-	17	4^2+1^2
6	-	12	-	18	3^2+3^2

Extracting the prime values $p = n$ from the previous table gives the following table.

p	$a^2 + b^2$	p	$a^2 + b^2$	p	$a^2 + b^2$
2	$1^2 + 1^2$	13	$3^2 + 2^2$	31	
3	-	17	$4^2 + 1^2$	37	
5	$2^2 + 1^2$	19		41	
7	-	23		43	
11	-	29		47	

Exercise: complete this table.

p	$a^2 + b^2$	p	$a^2 + b^2$	p	$a^2 + b^2$
2	$1^2 + 1^2$	13	$3^2 + 2^2$	31	-
3	-	17	$4^2 + 1^2$	37	$6^2 + 1^2$
5	$2^2 + 1^2$	19	-	41	$5^2 + 4^2$
7	-	23	-	43	-
11	-	29	$5^2 + 2^2$	47	-

Note the similarity to previous table with solutions of $x^2 \equiv -1 \pmod{p}$. It seems as if this congruence is soluble if and only if p is the sum of two squares. Indeed this is the case!

We prove that primes $p \equiv 3 \pmod 4$ cannot lie in S_2; indeed it is "difficult" for such a prime to divide an element of S_2.

Theorem 10 *Let p be a prime with $p \equiv 3 \pmod 4$. If $a, b \in \mathbf{Z}$ and $p \mid (a^2 + b^2)$ then both $p \mid a$ and $p \mid b$.*

Proof Let's assume that $p \nmid a$. Then there is a reciprocal of a modulo p, that is a number c with $ca \equiv 1 \pmod p$. Then $p \mid c^2(a^2 + b^2)$ and so

$$0 \equiv (ca)^2 + (cb)^2 \equiv 1 + (cb)^2 \pmod p.$$

This means that $x = cb$ is a solution of the congruence $x^2 \equiv -1 \pmod p$. But as $p \equiv 3 \pmod 4$ this congruence is insoluble. By contradiction then $p \mid a$. Similarly, $p \mid b$. □

As a consequence of this, if p is prime, $p \equiv 3 \pmod 4$, $n \in S_2$ and $p \mid n$ then $p^2 \mid n$; moreover $n/p^2 \in S_2$, since if we write $n = a^2 + b^2$ then $a = pr$ and $b = ps$ where $a, b \in \mathbf{Z}$ and $n/p^2 = r^2 + s^2 \in S_2$.

For example, $220 = 2 \times 5 \times 11 \notin S_2$ as 11 is prime, $11 \equiv 3 \pmod 4$, $11 \mid 220$ but $11^2 \nmid 220$.

Repeating the previous argument yields the following result, which states in effect that for n to lie in S_2 a prime congruent to 3 modulo 4 must divide it an even number of times.

Theorem 11 *Let p be a prime with $p \equiv 3 \pmod 4$ and $n \in S_2$. If we write $n = p^r m$ with $p \nmid m$ then r is even and $m \in S_2$.*

Proof We proceed by induction on r. There is nothing to prove when $r = 0$. Suppose that $r > 0$. Then by the previous remark, $p^2 \mid n$ and $n/p^2 \in S_2$. This means that $r \geq 2$ and $p^{r-2}m \in S_2$. By the inductive hypothesis, $r - 2$ is even and $m \in S_2$. It follows that r is even too. □

As an example, $1715 = 5 \times 7^3 \notin S_2$, as 7 is prime, $7 \equiv 3 \pmod 4$ and 7 divides 1715 an odd number of times.

So far we have lots of negative results about S_2: various criteria proving that numbers aren't sums of two squares. What about positive results? Can we describe any classes of numbers that are definitely sums of two squares?

One obvious result, that is too obvious to be called a theorem is that if $n \in S_2$ and $r \in \mathbf{Z}$ then $r^2 n \in S_2$, since $n = a^2 + b^2$ implies $r^2 n = (ra)^2 + (rb)^2$. For example, as $41 = 5^2 + 4^2 \in S_2$ then $4100 = 50^2 + 40^2 \in S_2$.

The real key to the structure of S_2 is the following theorem which is a massive generalization of the previous trite observation. It states in effect that S_2 is closed under multiplication.

Theorem 12 *Let $m \in S_2$ and $n \in S_2$. Then $mn \in S_2$.*

Proof It's convenient to use complex numbers. Write $m = a^2 + b^2$ and $n = c^2 + d^2$. Then $m = |\alpha|^2$ and $n = |\beta|^2$ where $\alpha = a + bi$ and $\beta = c + di$. So $mn = |\alpha|^2|\beta|^2 = |\alpha\beta|^2$. The complex number $\alpha\beta = r + si$ where r and s are real. Indeed r and s are integers, for $r = ac - bd$ and $s = ad + bc$. Hence $mn = r^2 + s^2 \in S_2$. □

A complex number of the form $a+bi$ where a and b are integers is called a *Gaussian integer*. If α is a complex number then $|\alpha|^2$ is called its *norm*. The norm of a product of two complex numbers is the product of their norms. The elements of S_2 are precisely the norms of Gaussian integers. As the product of two Gaussian integers is a Gaussian integers, then the product of two elements of S_2 is an element of S_2.

We can use the method of the proof to compute examples. Consider $9797 = 97 \times 101$. Now $97 = 9^2 + 4^2$ and obviously $101 = 10^2 + 1^2$. Thus

$$\begin{aligned} 9797 &= (9^2 + 4^2)(10^2 + 1^2) \\ &= |9 + 4i|^2 |10 + i|^2 \\ &= |(9 + 4i)(10 + i)|^2 \\ &= |86 + 49i|^2 \\ &= 86^2 + 49^2. \end{aligned}$$

Indeed by jiggling one of the complex numbers here we can get a different representation:

$$\begin{aligned} 9797 &= (9^2 + 4^2)(1^2 + 10^2) \\ &= |9 + 4i|^2 |1 + 10i|^2 \\ &= |(9 + 4i)(1 + 10i)|^2 \\ &= |-31 + 94i|^2 \\ &= 31^2 + 94^2. \end{aligned}$$