Last time we proved quadratic reciprocity (QR), which tells us whether or not a given quadratic congruence of the form

$$x^2 \equiv a \pmod{p} \tag{$*$}$$

is solvable. But how do we actually solve it? Our first goal is to outline a method of doing so.

In order to solve $(*)$ it needs to be solvable, so we may immediately assume $\left(\frac{a}{p}\right) = 1$. Thus by Euler's criterion we may safely assume

$$a^{(p-1)/2} \equiv 1 \pmod{p}. \tag{$\heartsuit$}$$

Now comes the key observation: if $\frac{p-1}{2}$ is odd, then we can multiply both sides by a to get

$$a^{\text{even}} \equiv a \pmod{p},$$

which immediately allows us to solve $(*)$!

Let's make this more precise. If $p \equiv -1 \pmod{4}$, then we can multiply both sides of $(\heartsuit)$ by a to obtain

$$a^{(p+1)/2} \equiv a \pmod{p}.$$

Since $p \equiv -1 \pmod{4}$, we find that

$$x \equiv \pm a^{(p+1)/4} \pmod{p}$$

are two distinct solutions to $(*)$. Are there other solutions? No, because by problem **6.4** the congruence $(*)$ has at most two solutions (mod p)! We can summarize the above in the following:

<u>Proposition:</u> If $p \equiv -1 \pmod{4}$ and $\left(\frac{a}{p}\right) = 1$, then the solutions to (*) are $\pm a^{(p+1)/4} \pmod{p}$.

What if $p \equiv 1 \pmod{4}$? Then the above doesn't work, since $(p-1)/2$ is already even, so multiplying both sides of $(\heartsuit)$ by a doesn't help. This does mean, however, that we can take square-roots of both sides of $(\heartsuit)$! We can then repeat a similar procedure as above, but considering $p \pmod{8}$. You will explore this approach on this week's problem set.

In view of the above, we can efficiently solve quadratic congruences (mod p)! Actually, this isn't quite true: we can solve congruences of the very special form $(*)$. What about the general quadratic congruence

$$ax^2 + bx + c \equiv 0 \pmod{p}? \tag{$\dagger$}$$

First observe that it suffices to consider quadratics of the form

$$x^2 + bx + c \equiv 0 \pmod{p}. \tag{$\ddagger$}$$

Indeed, given any congruence of the form (†), we might as well assume that $a \not\equiv 0 \pmod p$, since otherwise this is a linear congruence (and we know how to solve those). But if $a \not\equiv 0 \pmod p$ we can divide both sides by a to get a congruence of the form (‡) that has the same solutions as (†).

OK, so how do we solve (‡)? This is classical: complete the square! We see that (‡) implies

$$(x + \tfrac{b}{2})^2 \equiv x^2 + bx + (\tfrac{b}{2})^2 \equiv (\tfrac{b}{2})^2 - c \pmod p.$$

But this is precisely a congruence of the form ($*$), so we can solve for $x + \frac{b}{2}$! Thus, we have a method for solving arbitrary quadratic congruences (mod p).

Now what if we move away from (mod p) to (mod n)? For example, suppose we wish to solve

$$x^2 \equiv a \pmod{pq} \qquad (\clubsuit)$$

where p and q are distinct primes. It turns out we can solve this using the Chinese Remainder Theorem.

<u>Step 1:</u> Using our method above, find a solution to $x^2 \equiv a \pmod p$, say, $x \equiv x_p \pmod p$. Similarly, find a solution $x \equiv x_q \pmod q$ to $x^2 \equiv a \pmod q$.

<u>Step 2:</u> By CRT there exists a unique $y \in \mathbb{Z}_{pq}$ such that $y \equiv x_p \pmod p$ and $y \equiv x_q \pmod q$. Moreover, this y isn't hard to actually compute.

<u>Step 3:</u> We've thus found a number $y \in \mathbb{Z}_{pq}$ such that

$$y^2 \equiv x_p^2 \equiv a \pmod p \qquad \text{and} \qquad y^2 \equiv x_q^2 \equiv a \pmod q.$$

I claim this means $y^2 \equiv a \pmod{pq}$. Indeed, note that $a \equiv a \pmod p$ and $a \equiv a \pmod q$, and the CRT implies that a is the *unique* element of $\mathbb{Z}_{pq}$ satisfying this. But y^2 also satisfies these two congruences! Thus, $y^2 \equiv a \pmod{pq}$. Since we actually computed y, we've found a solution to ($\clubsuit$)!

This looks very nice, but there's an important subtlety: to make the above procedure work, we need to know p and q individually. In other words, if we can factor the composite number pq, then we can efficiently solve quadratic congruences (mod pq). It turns out the converse is also true: if there exists an efficient method to solve quadratic congruences (mod pq), then we can use it to efficiently determine the factorization of pq. Thus, solving quadratic congruences (mod pq) is comparably difficult to factoring! Since efficient factoring is currently open, so is the question of efficiently solving quadratic congruences (mod pq).

This concludes (for now) our exploration of the modular world, and we return to the familiar land of $\mathbb{Z}$.

Sums of Squares

Question: Which integers can be written as the sum of two squares? Put more formally: what can we say about the structure of the set

$$S := \{x^2 + y^2 : x, y \in \mathbb{Z}\} = \{0, 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29, 32 \dots\}?$$

Well, we know that n^2 and $n^2 + 1$ live in S for every integer n. But what about some random number? For example, is $2019 \in S$? Ben says no, because nothing $\equiv 3 \pmod 4$ lives in S. Why is this?

Proposition: Any perfect square is $\equiv 0$ or $1 \pmod 4$.
Proof: We have $(2n)^2 \equiv 0 \pmod 4$ and $(2n+1)^2 \equiv 1 \pmod 4$. Since any integer is even or odd, this proves the claim. □

Thus anything in S must be 0, 1, or 2 (mod 4); in particular, S does not contain any number that's 3 (mod 4). What about the converse? Is everything equivalent to 0, 1, or 2 (mod 4) in S? No: $6 \notin S$.

Since the structure of S is opaque, we turn to a related (but hopefully easier) problem to get inspired. Define

$$D := \{x^2 - y^2 : x, y \in \mathbb{Z}, x \geq y\} = \{0, 1, 3, 4, 5, 7, 8, 9, 11, 12, 13, \dots\}.$$

Max: All odd integers are in D since $2n + 1 = (n + 1 + n)(n + 1 - n) = (n + 1)^2 - (n)^2 \in D$.

If $n \equiv 2 \pmod 4$ then $n \notin D$, since any square is 0 or 1 (mod 4).

Oliver: $4n = (n + 1 + n - 1)(n + 1 - (n - 1)) = (n + 1)^2 - (n - 1)^2 \in D$.

Putting these three insights together, we see that $D = \{n \geq 0 : n \not\equiv 2 \pmod 4\}$.

Returning to S, we see that a similar trick doesn't work, since we can't factor the sum of two squares. OR CAN'T WE? Ben pointed out we can factor this in $\mathbb{C}$: $x^2 + y^2 = (x + iy)(x - iy)$. This led us to think about the 'Gaussian integers'

$$\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}.$$