26. 4/19

26.1. The notes for this day are longer than usual, to include supplementary material that would have been covered on Patriots' Day.

26.2. Last week, we learned an efficient algorithm to determine whether an integer a is a quadratic residue modulo an odd prime p. What about the quadratic residues modulo m for composite $m \in \mathbf{N}$?

As usual, the prime 2 causes complications, so for now, let's stick to odd m. The smallest composite odd number is $m = 9$. We compute:

$x \pmod 9$	0	± 1	± 2	± 3	± 4
$x^2 \pmod 9$	0	1	4	0	7

So the *nonzero* quadratic residues modulo 9 are $1, 4, 7$. We notice that these remainders form an arithmetic progression: In fact, they are precisely the remainders mod 9 that are congruent to 1 modulo 3.

At the same time, the only nonzero quadratic residue modulo 3 is 1. So for $a \not\equiv 0 \pmod 3$, we find that a is a QR modulo 9 if and only if a is a QR modulo 3. The analogue is true for other odd primes, and also for higher powers:

Theorem 26.1. *If $p > 0$ is an odd prime and $k \in \mathbf{N}$ and $a \not\equiv 0 \pmod{p^k}$, then*

$$a \text{ is a QR modulo } p^{k+1} \iff a \text{ is a QR modulo } p^k.$$

26.3. Which direction is easier to prove? If $x^2 \equiv a \pmod{p^{k+1}}$, then $x^2 \equiv a \pmod{p^k}$ because divisibility by p^k is weaker than divisibility by p^{k+1}. But the converse fails: $2^2 \equiv 1 \pmod 3$, but $2^2 \not\equiv 1 \pmod 9$. Nonetheless:

Lemma 26.2. *If $a \not\equiv 0 \pmod{p^k}$, and x_k is a solution to*

$$x_k^2 \equiv a \pmod{p^k}.$$

then there is some integer b such that $x_{k+1} = x_k + bp^k$ is a solution to

$$x_{k+1}^2 \equiv a \pmod{p^{k+1}}.$$

Proof. If $x_k \equiv 0 \pmod{p^k}$, then $a \equiv 0 \pmod{p^k}$, so we may assume that $x_k \not\equiv 0 \pmod{p^k}$ in what follows. We expand

$$x_{k+1}^2 = x_k^2 + 2x_k bp^k + b^2 p^{2k} \equiv x_k^2 + 2x_k bp^k \pmod{p^{k+1}},$$

using the fact that $2k \geq k + 1$. So it suffices to construct some b such that

$$x_k^2 + 2x_k bp^k \equiv a \pmod{p^{k+1}}.$$

Since p is odd and $x_k \not\equiv 0 \pmod{p^k}$, we can invert $2x_k$ modulo p^{k+1}: That is, $2x_k u \equiv 1 \pmod{p^{k+1}}$ for some integer u. So it suffices to construct b so that

$$bp^k \equiv (a - x_k^2)u \pmod{p^{k+1}}.$$

Such b exists, because the right-hand side vanishes modulo p^k. □

26.4. *Hensel's lemma* You can think of the argument above as studying the solutions of $x^2 - a = 0$ using "Taylor expansion in p". The argument can be generalize to show:

Theorem 26.3 (Hensel)**.** *Let $p > 0$ be prime, and let $f(x)$ be a polynomial with integer coefficients. If there exist $k \in \mathbf{N}$ and an integer x_k such that*

$$\begin{aligned} f(x_k) &\equiv 0 \pmod{p^k}, \\ f'(x_k) &\not\equiv 0 \pmod{p}, \end{aligned}$$

then there exists some integer x_{k+1} such that

$$f(x_{k+1}) \equiv 0 \pmod{p^{k+1}}.$$

Explicitly, if $f'(x_k)u \equiv 1 \pmod{p}$, then we set $x_{k+1} = x_k - f(x_k)u$.

26.5. The discussion above shows how to deal with quadratic residues modulo odd prime powers. As for other odd composite numbers:

Theorem 26.4. *If $m = m'm''$, where m' and m'' are relatively prime, and $a \not\equiv 0 \pmod{m}$, then*

$$a \text{ is a QR modulo } m \iff a \text{ is a QR modulo } m' \underline{\text{and}} \text{ modulo } m''.$$

Proof. By the Chinese Remainder Theorem, $(\mathbf{Z}/m\mathbf{Z})^\times$ under multiplication is isomorphic to $(\mathbf{Z}/m'\mathbf{Z})^\times \times (\mathbf{Z}/m''\mathbf{Z})^\times$ under coordinate-wise multiplication. □

So we can always reduce the case of an odd composite number to the case of an odd prime power, and from there, to the case of an odd prime. It's also easy to do $2m$, $4m$, and $8m$ for odd m, since 1 is the only nonzero quadratic residue modulo 2, 4, and 8.

Example 26.5. To check if something is a quadratic residue modulo 90, we just need to check modulo 2 and 5 and 9. To check the modulo-9 case, we just need to check modulo 3.

Higher powers of 2 are complicated, and I don't want to spend time on them in this course. But the theory has been worked out. For instance, it's known that if $a \equiv 1 \mod 8$, then a is a QR modulo 2^k for all $k \in \mathbf{N}$.

26.6. *Adjoining solutions* We've seen that the equation $x^2 - a \equiv 0 \pmod{m}$ does not always have solutions. The answer to whether or not solutions exist involves a rich interplay between the arithmetic of a and of m.

But this situation already happens in a more familiar number system: namely, the set of real numbers $\mathbf{R}$. We cannot solve $x^2 + 1 = 0$ for a real number x. Rather, we invent the complex numbers by *adjoining* a solution of this equation, which we call i, to the number system $\mathbf{R}$.

We want to extend the operations of addition and multiplication from $\mathbf{R}$ to $\mathbf{C}$, so that these operations remain associative and commutative, and so that multiplication still distributes over addition. Everything works if we define $\mathbf{C}$ as the set of formal sums $x + yi$, where $x, y \in \mathbf{R}$, and define our operations *in terms of* the distributive property. The big question is: Can we do a similar thing with the sets $\mathbf{Z}/m\mathbf{Z}$?

26.7. *Rings* Up till now, I have used the term "number system" in an informal way, but now we are forced to fix a precise definition.

Namely, a *commutative ring* is a set R together with two binary operations, called its *addition* $+$ and its *multiplication* $\cdot$, such that:

(1) $+$ and $\cdot$ are associative.
(2) $+$ and $\cdot$ are commutative. That is, $x + y = y + x$ and $x \cdot y = y \cdot x$.
(3) There is an element $0 \in R$ such that $x + 0 = x$ for all $x \in R$.
(4) There is an element $1 \in R$ such that $x \cdot 1 = x$ for all $x \in R$.
(5) For all $x \in R$, there is an element $-x \in R$ such that $x + (-x) = 0$.
(6) For all x, y, z, we have

$$\begin{aligned} x \cdot (y + z) &= x \cdot y + x \cdot z, \\ (y + z) \cdot x &= y \cdot x + z \cdot x. \end{aligned}$$

That is, $\cdot$ distributes over $+$ on both the left and the right.

The axioms above imply that R forms an abelian group under $+$. However, it need not form a group under $\cdot$, because we do not require that every element of R have an inverse under $\cdot$.

26.8. Henceforth, we will refer to commutative rings simply as *rings*. This is a serious abbreviation: In the literature, the term *ring* usually means the multiplication $\cdot$ is not required to be commutative. For intance, the set of $n \times n$ real matrices forms a ring in which multiplication is not commutative. However, in this course, all rings we study will be commutative.

26.9. When we study groups, the group operation could be addition, multiplication, or even something else. When we study rings, $+$ always denotes addition, and $\cdot$ always denotes multiplication. So we will not mention these symbols whenever we introduce a new ring.

26.10. We have seen many rings in this course:

$$\mathbf{Z}, \quad \mathbf{Q}, \quad \mathbf{R}, \quad \mathbf{C}, \quad \mathbf{Z}/m\mathbf{Z}, \quad \mathbf{Z}[i], \quad \mathbf{Z}[i]/\alpha\mathbf{Z}[i], \quad \mathbf{Z}[\omega], \quad \ldots$$

By contrast, $m\mathbf{Z}$ is not a ring when $m > 1$: only a group under addition.

26.11. *Units and fields* An element $x \in R$ is *invertible*, or a *unit*, iff it does have an inverse under multiplication: that is, an element $x^{-1} \in R$ such that $x \cdot x^{-1} = 1$.

Example 26.6. You can check that $x \cdot 0 = 0$ for all $x \in R$. Thus the only case where 0 is a unit is when $R = \{0\}$.

The set of units of R forms a group under multiplication, which we denote by $R^\times$. This notation generalizes our earlier notation $(\mathbf{Z}/m\mathbf{Z})^\times$.

We say that R is a *field* iff $R \neq \{0\}$ and every nonzero element is invertible: that is, $R^\times = R - \{0\}$. We immediately see that $\mathbf{Q}, \mathbf{R}, \mathbf{C}$ are fields. But if p is a prime, then the ring $\mathbf{Z}/p\mathbf{Z}$ also forms a field. In the literature, when people want to emphasize this fact, they will often write $\mathbf{F}_p$ in place of $\mathbf{Z}/p\mathbf{Z}$.

Suppose α is a Gaussian prime. Is it true that $\mathbf{Z}[i]/\alpha\mathbf{Z}[i]$ forms a field? It turns out that the answer is yes. One of the non-book problems on Problem Set 5 asks you to explore this fact for various α.

26.12. Recall that -1 is not a quadratic residue modulo 3. That is, there is no integer x such that $x^2 \equiv -1 \pmod{3}$. Yet there are indeed Gaussian integers such that $x^2 \equiv -1 \pmod{3}$: namely, $x = \pm i$.

In other words, we cannot solve $x^2 + 1 = 0$ in the ring $\mathbf{Z}/3\mathbf{Z}$, but we can in the larger ring $\mathbf{Z}[i]/3\mathbf{Z}[i]$. This is exactly analogous to how we cannot solve this equation in $\mathbf{R}$, but can in $\mathbf{C}$.

What about $\mathbf{Z}[i]/5\mathbf{Z}[i]$? Here there are actually four distinct solutions to $x^2 + 1 = 0$: namely, $x \equiv \pm 2, \pm i \pmod{5}$. This hints at a serious structural difference between $\mathbf{Z}[i]/3\mathbf{Z}[i]$ and $\mathbf{Z}[i]/5\mathbf{Z}[i]$. We will find that the former is a field, but the latter is not.