Topics: Quadratic residues etc.

5.1. Fix an odd prime p.
Prove that there are exactly $(p-1)/2$ quadratic residues modulo p.

Solution. Let g be a primitive root modulo p. Every $a \in (\mathbf{Z}/p\mathbf{Z})^\times$ can be written uniquely as $a \equiv g^e \pmod{p}$ for some e such that $0 \leqslant e < p-1$.

We have seen that a is a quadratic residue if and only if e is even. So the number of quadratic residues is the number of even integers e such that $0 \leqslant e < p-1$, which is $(p-1)/2$. □

5.2 (Euler's Criterion)**.** Fix an odd prime p and an integer a.

(a) Prove that $a^{(p-1)/2} \equiv -1, 0, 1 \pmod{p}$.

(b) Prove that $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$.

(c) What does the previous part say in the case $a = -1$? Does this look familiar?

Solution.

(a) If $p \mid a$ then $a^{(p-1)/2} \equiv 0 \pmod{p}$.

If $p \nmid a$ then, by Fermat's little Theorem, $a^{p-1} \equiv 1 \pmod{p}$. Let $t = a^{(p-1)/2} \pmod{p}$. Then $t^2 \equiv 1 \pmod{p}$, so $t \equiv \pm 1 \pmod{p}$ since: p is prime so $\mathbf{Z}/p\mathbf{Z}$ is a field, hence the quadratic polynomial $t^2 - 1$ has at most two roots, but ± 1 are clearly roots and $1 \neq -1$ as p is odd.

(b) If $p \mid a$ then the two sides of the congruence are clearly 0.

Now it suffices to prove that a is a quadratic residue if and only if $a^{(p-1)/2} \equiv 0 \pmod{p}$.

In one direction, if $x^2 \equiv a \pmod{p}$, then $a^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod{p}$ by Fermat's little Theorem.

In the other direction, suppose $a^{(p-1)/2} \equiv 1 \pmod{p}$. Let g be a primitive root modulo p, then $a \equiv g^e \pmod{p}$ for some e with $0 \leqslant e < p-1$. Therefore $g^{e(p-1)/2} \equiv a^{(p-1)/2} \equiv 1 \pmod{p}$, but g has order $p-1$, so $(p-1) \mid e(p-1)/2$, forcing e to be even. We conclude that a is a quadratic residue.

(c) For $a = -1$ we get

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod{p}.$$

Since both sides can only be 1 or -1, we see that this is actually an equality of integers:

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2},$$

which we recognise as being part of the Quadratic Reciprocity Theorem. □

5.3.

(a) Prove that if $m \mid n$ and a is a quadratic residue modulo n then a is a quadratic residue modulo m.

(b) Conclude that if $m \mid n$ and a is a quadratic non-residue modulo m then a is a quadratic non-residue modulo n.

(c) Suppose $\gcd(m_1, m_2) = 1$ and a is both a quadratic residue modulo m_1 and a quadratic residue modulo m_2. Prove that a is a quadratic residue modulo $m_1 m_2$.

(d) Suppose $\gcd(m_1, m_2) = 1$. Based on the previous parts, complete the following to a true statement: "a is a quadratic residue modulo $m_1 m_2$ if and only if ……"

(e) Using your statement in (d), predict the list of quadratic residues modulo 15, based on the lists of quadratic residues modulo 3 and modulo 5.

Then compute (by brute force) the quadratic residues modulo 15 to check your list.

Solution.

(a) Suppose a is a quadratic residue modulo n. Then $\gcd(a, n) = 1$ and there exists x with $\gcd(x, n) = 1$ such that $x^2 \equiv a \pmod{n}$.

Since $m \mid n$, we have that $\gcd(a, m) = 1$. Also $m \mid n \mid (x^2 - a)$, therefore $x^2 \equiv a \pmod{m}$, so a is a quadratic residue modulo m.

(b) This is the contrapositive of part (a), hence equivalent to it.

(c) Let x_1 be such that $x_1^2 \equiv a \pmod{m_1}$ and let x_2 be such that $x_2^2 \equiv a \pmod{m_2}$.

Since $\gcd(m_1, m_2) = 1$, the Chinese Remainder Theorem says that the system of congruences

$$\begin{aligned} y &\equiv x_1 \pmod{m_1} \\ y &\equiv x_2 \pmod{m_2} \end{aligned}$$

has a unique solution modulo $m_1 m_2$.

The uniqueness part of the Chinese Remainder Theorem for the system

$$\begin{aligned} y^2 &\equiv x_1^2 \equiv a \pmod{m_1} \\ y^2 &\equiv x_2^2 \equiv a \pmod{m_2} \end{aligned}$$

now tells us that $y^2 \equiv a \pmod{m_1 m_2}$, hence a is a quadratic residue modulo $m_1 m_2$.

(d) "a is a quadratic residue modulo $m_1 m_2$ if and only if a is a quadratic residue modulo m_1 and modulo m_2."

(e) The only quadratic residue modulo 3 is 1. The quadratic residues modulo 5 are $1, 4$.

So the quadratic residues modulo 15 should be the integers $1 \leqslant a < 15$ such that $a \equiv 1 \pmod{3}$ and $a \equiv 1, 4 \pmod{5}$. This gives us $\{1, 4\}$.

We check this directly. Modulo 15, we have $1^2 \equiv 4^2 \equiv 11^2 \equiv 14^2 \equiv 1$, $2^2 \equiv 7^2 \equiv 8^2 \equiv 13^2 \equiv 4$, so the quadratic residues are $1, 4$. □

5.4. Consider the Goldwasser–Micali probabilistic one-bit encryption scheme.

(a) Prove that the Jacobi symbol $\left(\frac{c}{N}\right)$ is 1 no matter what the plaintext message m is, so Eve gets no useful information from computing it.

The setup of the scheme requires Bob to choose large random primes p and q (which we have discussed in the context of the RSA cryptosystem), then to find an integer b that is a quadratic non-residue modulo p and modulo q.

We explore some ways of getting a quadratic non-residue.

To start with, recall from Tutorial Question 5.2 that if $p \equiv 3 \pmod 4$, then -1 is a quadratic non-residue.

So assume now that $p \equiv 1 \pmod 4$.

In particular, -1 is a quadratic residue modulo p, so there exists i such that $i^2 \equiv -1 \pmod p$.

(b) Show that if $p \equiv 2 \pmod 3$, then 3 is a quadratic non-residue.

(c) Show that if $p \not\equiv 1 \pmod 8$, then i is a quadratic non-residue.

(d) Show that if $p \equiv 1 \pmod 8$ but $p \not\equiv 1 \pmod{16}$, then $(1+i)/\sqrt{2}$ is a quadratic non-residue.

(What does $\sqrt{2}$ mean here?)

(e) Describe a practical method for Bob to find a quadratic non-residue b modulo p and modulo q that works for many possible pairs (p, q) with $p \neq q$ odd primes.

(f) (just for fun) Can you estimate the proportion of pairs (p, q) for which the method works?

You may use the following (non-trivial) fact: for any positive integer m and any a with $\gcd(a, m) = 1$, the proportion of primes p such that $p \equiv a \pmod m$ is equal to $\phi(m)$.

Solution.

(a) If Alice's message is $m = 0$, then $c = r^2$ and

$$\left(\frac{c}{N}\right) = \left(\frac{r^2}{N}\right) = 1.$$

If $m = 1$, then $c = br^2$ and

$$\left(\frac{c}{N}\right) = \left(\frac{br^2}{N}\right) = \left(\frac{b}{N}\right)\left(\frac{r^2}{N}\right) = \left(\frac{b}{N}\right) = \left(\frac{b}{p}\right)\left(\frac{b}{q}\right) = (-1)(-1) = 1.$$

So even though Eve can compute the Jacobi symbol $\left(\frac{c}{N}\right)$ efficiently, its value is always 1, so it tells her nothing about the message m.

(b) Since $p \equiv 1 \pmod 4$ we have, by Quadratic Reciprocity:

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

(c) Suppose i is a quadratic residue, and fix j such that $j^2 \equiv i \pmod p$. Then $j^8 \equiv i^4 \equiv 1 \pmod p$, hence $8 \mid (p-1)$, contradicting the fact that $p \not\equiv 1 \pmod 8$.

(d) If $p \equiv 1 \pmod 8$ then by Quadratic Reciprocity 2 is a quadratic residue modulo p, hence there exists an integer that we denote $\sqrt{2}$ with the property that $(\sqrt{2})^2 \equiv 2 \pmod p$. (For instance, if $p = 17$ then $6^2 \equiv 2 \pmod{17}$, so we could take $\sqrt{2} = 6$ in this case.)

Suppose $(1+i)/\sqrt{2}$ is a quadratic residue, and fix k such that $k^2 \equiv (1+i)/\sqrt{2} \pmod p$. Then $k^4 \equiv (1+i)^2/2 \equiv 2i/2 \equiv i \pmod p$, so $k^16 \equiv i^4 \equiv 1 \pmod p$, so $16 \mid (p-1)$, contradiction.

(e) Bob could choose each of the primes p and q to belong to one of the sets of primes for which we have identified a quadratic non-residue, that is:

$$\begin{aligned} S_1 &= \{p : \ p \equiv 3 \pmod 4\}, \\ S_2 &= \{p : \ p \equiv 1 \pmod 4 \text{ and } p \equiv 2 \pmod 3\}, \\ S_3 &= \{p : \ p \equiv 1 \pmod 4 \text{ and } p \not\equiv 1 \pmod 8\}, \\ S_4 &= \{p : \ p \equiv 1 \pmod 8 \text{ and } p \not\equiv 1 \pmod{16}\}, \end{aligned}$$

then use the Chinese Remainder Theorem to produce an integer b that is a quadratic non-residue for both p and q.

(f) Estimating the proportions is easier if all congruences are modulo the same integer, so we will take the least common multiple 48 of the moduli in part (e) and rewrite our sets:

$$\begin{aligned} S_1 &= \{p \equiv 3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47 \pmod{48}\}, \\ S_2 &= \{p \equiv 5, 17, 29, 46 \pmod{48}\}, \\ S_3 &= \{p \equiv 5, 13, 21, 29, 37, 45 \pmod{48}\}, \\ S_4 &= \{p \equiv 9, 25, 41 \pmod{48}\}. \end{aligned}$$

We remove the cases that are not coprime to 48 as well as the repetitions and are left with the congruence classes

$$\{5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47\}.$$

That's 15 classes out of a total of $\phi(48) = 16$.

So the proportion of pairs for which the method works is $(15/16)^2 \approx 88\%$. □

5.5. Fix a prime $p \geqslant 5$. A *cubic residue modulo p* is an element $a \in (\mathbf{Z}/p\mathbf{Z})^\times$ such that the congruence $x^3 \equiv a \pmod p$ is solvable.

(a) Find the cubic residues and modulo 7; modulo 11; modulo 13.

(b) Show that if $p \equiv 2 \pmod 3$ then the function $F : \ (\mathbf{Z}/p\mathbf{Z})^\times \longrightarrow (\mathbf{Z}/p\mathbf{Z})^\times$ given by $F(x) = x^3$ is a bijection. Therefore every element of $(\mathbf{Z}/p\mathbf{Z})^\times$ is a cubic residue.

(c) Suppose $p \equiv 1 \pmod 3$ and let g be a primitive root modulo p. Prove that a is a cubic residue modulo p if and only if $a \equiv g^e \pmod p$, where $3 \mid e$.

(d) Continuing to assume that $p \equiv 1 \pmod 3$, what can you say about the cubic residueness of:

- the product of two cubic residues;
- the product of two cubic non-residues;
- the product of a cubic residue and a cubic non-residue?

Solution.

(a) Modulo 7: the cubic residues are 1 and 6.

Modulo 11: every element is a cubic residue $1, 2, 3, \ldots, 10$.

Modulo 13: the cubic residues are $1, 5, 8, 12$.

(b) The given function F is a group homomorphism. Since the domain and codomain are the same (and finite), it suffices to prove that F is injective, that is $\ker F = \{1\}$.

So let $x \in \ker F$: $x^3 \equiv 1 \pmod{p}$. Let g be a primitive root modulo p and let $e = \log_g(x)$, so that $g^e \equiv x \pmod{p}$. Then $g^{3e} \equiv x^3 \equiv 1 \pmod{p}$, so $3e \equiv 0 \pmod{p-1}$.

Since $p \equiv 2 \pmod{3}$, $3 \nmid (p-1)$, so 3 is invertible mod $p-1$ and we conclude that $e \equiv 0 \pmod{p-1}$. But then $x \equiv g^e \equiv 1 \pmod{p}$, as we wanted to show.

(c) If $3 \mid e$, say $e = 3k$, then $a \equiv g^e \equiv (g^k)^3 \pmod{p}$ is a cubic residue modulo p.

Conversely, suppose a is a cubic residue, so there exists x such that $x^3 \equiv a \equiv g^e \pmod{p}$.

Let $f = \log_g(x)$, then $g^{3f} \equiv x^3 \equiv g^e \pmod{p}$, hence $3f \equiv e \pmod{p-1}$.

As $p \equiv 1 \pmod{3}$, $p-1$ is a multiple of 3, and since $3f$ is a multiple of 3, we must have that e is a multiple of 3.

(d) We use part (c).

If a and b are cubic residues, so that $a \equiv g^{3e} \pmod{p}$ and $b \equiv g^{3f} \pmod{p}$, then $ab \equiv g^{3(e+f)} \pmod{p}$, hence ab is a cubic residue.

Similarly, if a is a cubic residue and b is a cubic non-residue, so that $a = g^{3e}$ and $b = g^f$ with $f \not\equiv 0 \pmod{3}$, then $ab = g^{3e+f}$ with $3e + f \equiv f \not\equiv 0 \pmod{3}$, hence ab is a cubic non-residue.

On the other hand the product of two cubic non-residues may or may not be a cubic residue. For instance, modulo 13, both 2 and 4 are cubic non-residues, and $8 = 2 \cdot 4$ is a cubic residue. But 2 and 3 are cubic non-residues, and $6 = 2 \cdot 3$ is a cubic non-residue. □

5.6. Fix a prime $p \equiv 3 \pmod{4}$ and suppose a is a quadratic residue modulo p.
Prove that $x \equiv a^{(p+1)/4}$ is a solution of the congruence $x^2 \equiv a \pmod{p}$.
(In other words: this is a setting in which taking the square root modulo p is very easy.)

Solution. We have

$$x^2 \equiv a^{(p+1)/2} \equiv a \cdot a^{(p-1)/2} \equiv a \cdot \left(\frac{a}{p}\right) \equiv a \pmod{p}. \qquad \square$$