Topics: Quadratic residues etc..

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

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?

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.

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 $\phi(m)$.

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?

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.)