Math 345 – Monday 11/06/17

Exercise 37. For each odd prime p, we consider the two numbers

$$A = \text{ sum of all } 1 \le a < p \text{ such that } a \text{ is a quadratic residue modulo } p,$$

$$B = \text{ sum of all } 1 \le a < p \text{ such that } a \text{ is a nonresidue modulo } p.$$

For example, if $p = 11$, then the quadratic residues are

$$1^2 \equiv 1 \pmod{11}, \qquad 2^2 \equiv 4 \pmod{11}, \qquad 3^2 \equiv 9 \pmod{11},$$
$$4^2 \equiv 5 \pmod{11}, \qquad \text{and} \qquad 5^2 \equiv 3 \pmod{11}.$$

So

$$A = 1 + 4 + 9 + 5 + 3 = 22 \qquad \text{and} \qquad B = 2 + 6 + 7 + 8 + 10 = 33.$$

(a) Make a list of the quadratic residues for all odd primes $p < 20$.
(b) Add to your list A, B, and $A + B$ for all odd primes $p < 20$.
(c) What is the value of $A + B$ in general?
(d) Use induction on positive integers n to prove that

$$1^2 + 2^2 + \cdots + n^2 = n(n+1)(2n+1)/6.$$

(e) Compute $A \pmod p$ and $B \pmod p$. Find a pattern and use the previous part to prove that it is correct.
(f) Show that if $p \equiv_4 1$, and $n_1, \ldots, n_r$ are the numbers between 1 and $(p-1)/2$ that are residues modulo p, then $n_1, \ldots, n_r, p - n_r, \ldots, p - n_1$ is the complete set of residues modulo p.
(g) Use the previous parts to show that if $p \equiv_4 1$, then $A = B$.

Exercise 38. Determine whether each of the following congruences has a solution. (All of the moduli are primes.)
(a) $x^2 \equiv -1 \pmod{5987}$
(b) $x^2 \equiv 6780 \pmod{6781}$
(c) $x^2 + 14x - 35 \equiv 0 \pmod{337}$
(d) $x^2 - 64x + 943 \equiv 0 \pmod{3011}$
[Hint. For (c), use the quadratic formula to find out what number you need to take the square root of modulo 337, and similarly for (d).]