ANSWERS
Math 345
Homework 10
11/15/2017

Note: brief answers are given in places instead of full solutions.

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 $p < 20$

See below.

(b) Add to your list A, B, and $A + B$ for all odd primes $p < 20$.

p	residues	A	B	$A+B$
3	1	1	2	3
5	$1, 4$	5	5	10
7	$1, 2, 4$	7	14	21
11	$1, 3, 4, 5, 9$	11	44	55
13	$1, 3, 4, 9, 10, 12$	39	39	78
17	$1, 2, 4, 8, 9, 13, 15, 16$	68	68	136
19	$1, 4, 5, 6, 7, 9, 11, 16, 17$	76	95	171

(c) What is the value of $A + B$ in general?

We have

$$A + B \equiv_p \sum_{k=1}^{p-1} k = \frac{(p-1)p}{2}.$$

Note that this is a multiple of p (since $p - 1$ is even, so that $(p - 1)/2 \in \mathbb{Z}$). Therefore $A + B$ is always congruent to $0 \pmod{p}$.

(d) Use induction on positive integers n to prove that

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

Proof. For $n = 1$, we have $1(1+1)(2*1+1)/6 = 1*2*3/6 = 1 = 1^2$, as desired.

Now fix n, and assume $1^2 + 2^2 + \cdots + n^2 = n(n+1)(2n+1)/6$. Then

$$\begin{aligned} 1^2 + 2^2 + \cdots + n^2 + (n+1)^2 &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= \frac{2n^3 + 3n^2 + n + 6(n^2 + 2n + 1)}{6} \\ &= \frac{2n^3 + 9n^2 + 13n + 6)}{6} \\ &= \frac{(n+1)(n+2)(2n+3)}{6} \\ &= \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6}, \end{aligned}$$

as desired. So our equality holds for $n \geq 1$ by induction. □

(e) Compute $A \pmod p$ and $B \pmod p$. Find a pattern and use the previous part to prove that it is correct.

Answer. By the previous part, we have

$$A \equiv_p 1^2 + 2^2 + \cdots + \left(\frac{p-1}{2}\right)^2 \equiv_p \frac{1}{6}\frac{p-1}{2}\left(\frac{p+1}{2}\right)p.$$

For $p > 3$, $\gcd(6, p) = 1$, so that $\frac{1}{6}\frac{p-1}{2}\left(\frac{p+1}{2}\right) \in \mathbb{Z}$, and A is a multiple of p. So $A \equiv_p 0$.

For $p = 3$, we already computed $A = 1$ (which matches our formula here too).

Now, since $A + B \equiv_p 0$ (seen above), this means that B must also be congruent to 0 mod p (except of course when $p = 3$, which is computed explicitly above). □

(f) Show that if $p \equiv_4 1$, and $n_1, \dots, n_r$ are the numbers between 1 and $(p-1)/2$ that are residues modulo p, then $n_1, \dots, n_r, p - n_r, \dots, p - n_1$ is the complete set of residues modulo p.

Proof. If a is a quadratic residue, then $a \equiv_p b^2$ for some b. Also, if $p \equiv_4 1$, then -1 is a quadratic residue, i.e. there is some ϵ for which $\epsilon^2 \equiv_p -1$. So

$$p - a \equiv_p -a \equiv_p \epsilon^2 b^2 = (\epsilon b)^2.$$

So $p - a$ is also a quadratic residue. In particular, the map $x \mapsto p - x$ gives a bijection between the numbers between 1 and $(p-1)/2$ that are residues modulo p and the numbers between $(p+1)/2$ and p that are residues modulo p (it is bijective because it is its own inverse). So if $n_1, \dots, n_r$ are the numbers between 1 and $(p-1)/2$ that are residues modulo p, then $n_1, \dots, n_r, p - n_r, \dots, p - n_1$ is the complete set of residues modulo p. □

(g) Use the previous parts to show that if $p \equiv_4 1$, then $A = B$.

Proof. If $p \equiv_4 1$, then

$$A = n_1 + \cdots + n_r + (p - n_r) + \cdots + (p - n_1) = \left(\frac{p-1}{4}\right)p = \frac{1}{2}\left(\frac{(p-1)p}{2}\right) = \frac{A+B}{2}.$$

So $A = B$.

□

Exercise 38. Determine whether each of the following congruences has a solution. (All of the moduli are primes.)

(a) $x^2 \equiv -1 \pmod{5987}$ $\quad$ $5987 \equiv_4 -1$, so there is no solution.

(b) $x^2 \equiv 6780 \pmod{6781}$

Note $6780 \equiv -1 \pmod{6781}$. There is a solution, since $6781 \equiv 1 \pmod 4$. The solutions are $x \equiv 995$ and $x \equiv 5786$ modulo 6781.

(c) $x^2 + 14x - 35 \equiv 0 \pmod{337}$

Using the quadratic formula, the solutions are $x \equiv \frac{1}{2}(-14 \pm \sqrt{336})$. We know 2 is invertible, since it's relatively prime to 337. So we just need to know if 336 (i.e. -1) has a square root modulo 337. It does, since $337 \equiv 1 \pmod 4$, and so there is a solution. In fact, $148^2 \equiv -1 \pmod{337}$ and $189^2 \equiv -1 \pmod{337}$, so the original problem has solutions $x \equiv 67 \pmod{337}$ and $x \equiv 256 \pmod{337}$.

(d) $x^2 - 64x + 943 \equiv 0 \pmod{3011}$

This time the quadratic formula gives $x \equiv \frac{1}{2}(64 \pm \sqrt{324}$. Here, $324 = 18^2$ (as integers!), so $x = 23$ and 41 are actually roots of the polynomial $x^2 - 64x + 943$ (not just modulo 3011).

Exercise 39. Use the Law of Quadratic Reciprocity to decide whether a is a square mod b.

(a) $a = 85$, $b = 101$ $\quad$ Yes

(b) $a = 29$, $b = 541$ $\quad$ No

(c) $a = 101$, $b = 1987$ $\quad$ Yes

(d) $a = 31706$, $b = 43789$ $\quad$ No

Exercise 40. Does the congruence

$$x^2 - 3x - 1 \equiv 0 \pmod{31957}$$

have any solutions?

Yes, since $(-3)^2 - 4(1)(-1) = 13$, and $(\frac{13}{31957}) = 1$.

Exercise 41. Let p be a prime satisfying $p \equiv -1 \pmod 4$ and suppose that a is a quadratic residue modulo p.

(a) Show that $x = a^{(p+1)/4}$ is a solution to the congruence $x^2 \equiv a \pmod p$.
(This gives an explicit way to find square roots modulo p for primes congruent to $-1 \pmod 4$.)

We have

$$x^2 = (a^{(p+1)/4})^2 = a^{(p+1)/2} = a(a^{(p-1)/2}) \equiv_p a(\frac{a}{p}) = a,$$

where the second to last equality is by Euler's critereon, and the last is because a is a QR.

(b) Find a solution to the congruence $x^2 \equiv 7 \pmod{787}$.
(Your answer should lie between 1 and 786.)

By the previous part, one solution is $x = 7^{(787+1)/4} = 7^{197}$. To reduce this, we can use the method of successive squaring to get $x \equiv_{787} 105$.