# MATH 3320, HOMEWORK #7 – SOLUTIONS

DUE MONDAY, OCTOBER 15

**1.** (15 points) Use Euler's criterion to determine if 2 and 3 are squares modulo 79.

**Solution:** We must find $2^{39} \pmod 79$ and $3^{39} \pmod 79$ and determine whether they are 1 or $-1$.

We evaluate these by repeated squaring (you should show work to at least around the level of detail given below):

$2^1 \equiv 2$, $2^2 \equiv 4$, $2^4 \equiv 16$, $2^8 \equiv 19$, $2^{16} \equiv 45$, $2^{32} \equiv 50$

Now $(2^1)(2^2)(2^4)(2^{32}) = 1$, so 2 is a square.

$3^1 \equiv 3$, $3^2 \equiv 9$, $3^4 \equiv 2$, $3^8 \equiv 4$, $3^{16} \equiv 16$, $3^{32} \equiv 19$

Now $(2^1)(2^2)(2^4)(2^{32}) = -1$, so 3 is not a square.

**2.** (15 points) We know that if $p$ is a prime, then there exists a primitive root modulo $p$. Use this fact to give a direct proof that $(\frac{-3}{p}) = 1$ when $p \equiv 1 \pmod 3$. (Hint: There is an element $m \in (\mathbf{Z}/p\mathbf{Z})^\times$ of order 3. Show that $(2m+1)^2 \equiv -3$.)

**Solution:** We are given $p \equiv 1 \pmod 3$. We first show that there exists an element $m$ of order 3 modulo $p$.

Take $a$ to be a primitive root mod $p$. Since $p$ may be written in the form $3k+1$, we may set $m = a^k$. Now certainly $(a^k)^3 \equiv 1 \pmod p$. On the other hand if $a^k$, when raised to a power less than 3, were to become congruent to 1 mod $p$, it would follow that $a$ to a power of less than $3k$ would be congruent to 1, contradicting the fact that $a$ is a primitive root. It follows that $a^k$ has order exactly 3. Alternatively, we may simply note that $3|p-1$ and apply problem 1 from the last homework.

Now we have that $p$ divides $m^3-1$. Since $m^3-1$ factors as $(m-1)(m^2+m+1)$, it follows that $p$ must divide either $m-1$ or $m^2+m+1$. Since $m \not\equiv 1 \pmod p$, it follows that $p|m^2+m+1$. Thus $m^2+m+1 \equiv 0$. Now observe that we may write $(2m+1)^2 \equiv 4m^2+4m+1 \equiv 4(m^2+m+1)-3 \equiv -3 \pmod p$. It follows that $-3$ is a quadratic residue mod $p$.

**3.**

(a) (10 points) Fix a prime $p \equiv 3 \pmod 4$ and an integer $a$ that is a quadratic residue modulo $p$. Prove that $a^{(p+1)/4}$ is a solution to the congruence

$$x^2 \equiv a \pmod p.$$

*Proof.* If $(a,p) = 1$, then suppose

$$a \equiv g^2 \pmod p$$

for some $g$. Then

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

Thus

$$\left(a^{(p+1)/4}\right)^2 \equiv a^{(p+1)/2} \equiv a^{(p-1)/2} \cdot a \equiv 1 \cdot a \equiv a \pmod p.$$

If $(a,p) = p$, then

$$\left(a^{(p+1)/4}\right)^2 \equiv 0 \equiv a \pmod{p}.$$

$\square$

**Comment:** Legendre symbol can take 1, $-1$ or 0. The last case, where $(a,p) = p$ and $\left(\frac{a}{p}\right) = 0$, is likely to be missed.

(b) (10 points) Use part (a) to solve the equation $x^2 \equiv 37 \pmod{127}$.

**Solution:** 127 is prime. Use Euler's criterion,

$$37^{(127-1)/2} \equiv 37^{63} \equiv 1 \pmod{127}$$

So 37 is a quadratic residue modulo 127. Because $127 \equiv 3 \pmod 4$, according to (a), the solution to $x^2 \equiv 37 \pmod{127}$ is

$$x \equiv 37^{(127+1)/4} \equiv 37^{32} \equiv 37^{2^5} \equiv 52 \pmod{127}$$

Another solution is

$$127 - 52 \equiv 75 \pmod{127}$$

There are two solutions: 52 and 75.

**Comment:** You need to check the conditions $p \equiv 3 \pmod 4$ and "$a$ is a quadratic residue". There are two solutions of the quadratic modulo equation.

**4.** (20 points) Fix an odd prime $p$. Let $n$ be the smallest positive integer that is not a square modulo $p$. Prove that $n$ is a prime.

**Solution:** Suppose not. Since $n$ cannot be 1 (as this is obviously a square), $n$ must be composite. Thus it may be written in the form $n = ab$, where $a, b < n$. Now by the definition of $n$, we have $\left(\frac{n}{p}\right) = -1$ but $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1$. The multiplicativity of the Legendre symbol, however, implies that $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{n}{p}\right)$. This gives a contradiction. We conclude that $n$ must be prime.

**5.** (Extra Credit) Suppose that a teacher proposes to his $n$ students at recess that they play the following game. The $n$ children are to sit in a circle, and are numbered $0, \ldots, n-1$ clockwise. Their teacher walks clockwise around the children and hands out gumballs from a seemingly inexhaustible bag according to the following rule:

The teacher first select one child ("0") and gives them a gumball. Then he skips a child ("1") and gives a gumball to the next child ("2"). Then he skips 2 children ("3" and "4") and gives a gumball to the next one ("5"). Then he skips 3... etc.

(a) (5 points) What are the values of $n$ for which eventually (maybe after many rounds) each child ends up with at least one gumball? Furthermore, for such an $n$, how many gumballs need to be passed out? (Hint: Turn into a problem modulo $n$. What is $\sum_{k=1}^{m} k$ for various values of $m$?)

**Further Hint:** The gumballs end up at 0 and numbers of the form $S(m) = \frac{(m+2)(m-1)}{2}$ $(mod\ n)$. You need to determine for what values of $n$ the equation $S(m) \equiv \alpha$ $(mod\ n)$ has a solution for every $\alpha$. Use the Chinese remainder theorem, and your knowledge about solving quadratic equations. After that, do an example, and analyze $S(m_1) \equiv S(m_2)$.

**Solution:** The $m$th gumball will be given to the child congruent to $S(m) = \frac{(m+2)(m-1)}{2} \pmod n$. To ensure every child gets gumballs, $S(m) \equiv \alpha \pmod n$ should have solution for every $\alpha$. Suppose $n = p_1^{e1} \cdot \cdots \cdot p_k^{e_k}$ where $p_i$ for $i = 1, \cdots, k$ are distinct prime numbers and $e_i > 0$. Then

$$S(m) \equiv \alpha \pmod{p_i},\ i = 1, \cdots k$$

have solution for every $\alpha$. Because $S(m)$ is quadratic, when $p_i$ is odd, there exists $\alpha$ making the equation having no solution. Therefore, $n$ can only be a power of 2.

When $n = 2^e$, we can prove everyone can get gumballs by showing

$$\frac{(m+2)(m-1)}{2} \equiv \alpha \pmod{2^e}$$

has solution for every $\alpha$, which is equivalent to

$$m^2 + m - 2 - 2\alpha \equiv 0 \pmod{2^{e+1}}$$

has solution for every $\alpha$. Let $f(m) = m^2 + m - 2 - 2\alpha$. Then $f'(m) = 2m + 1 \equiv 1 \pmod 2$. According to Hensel's lemma, the modular equation always has solutions.

Last, we prove $2n - 1$ gumballs need to be passed out. Let $\alpha \equiv -1 \pmod 2$, consider

$$\frac{(m+2)(m-1)}{2} \equiv -1 \pmod{2^e}.$$

Then

$$m(m+1) \equiv (m+2)(m-1) + 2 \equiv 0 \pmod{2^{e+1}}$$

Since $m$ and $m+1$ are relatively prime, one of them must be a multiple of $2^{e+1}$:

$$m \equiv 0 \pmod{2^{e+1}} \text{ or } m \equiv -1 \equiv 2^{e+1} - 1 \pmod{2^{e+1}}$$

So for child number $n - 1$, the first gumball he/she gets is the $2^{e+1} - 1 = 2n - 1$th gumball.

(b) (5 points) Suppose you already know about this game (you're a transfer student and they played it at your old school), know that a total of $n$ students will be playing, and know that your teacher will always start by giving the person closest to the door a gumball. What position (of $\{0, 1, \ldots, n-1\}$) should you pick, if you want to get the most gumballs? Does it depend on how many gumballs are passed out? (e.g. if the teacher stops after $n$ gumballs, or after $\frac{n}{10}$ gumballs, or stops after everybody gets one, or hands out gumballs forever?)

**Further Hint:** Here $n$ is arbitrary. Use the Chinese Remainder Theorem.

**Solution:** For student numbered as $\alpha$, consider the number of solutions of

$$\frac{(m+2)(m-1)}{2} \equiv \alpha \pmod n$$

$$m^2 + m - 2 - 2\alpha \equiv 0 \pmod{2n}$$

Suppose $m_1$, $m_2$ are both solutions, we have

$$(m_1 - m_2)(m_1 + m_2 + 1) \equiv 0 \pmod{2n}$$

Suppose $C(m)$ is the child get the $m$th gumball. We claim $C(m)$ has period $n$ if $n$ is odd, and period $2n$ if $n$ is even. That is because if $m_1 = m_2 + n$, $n | m_1 - m_2$, and if $n$ is odd, then $m_1 + m_2 + 1 = 2m_2 + n + 1$ is even, so $2n | (m_1 - m_2)(m_1 + m_2 + 1)$. If $n$ is even, then $m_1 + m_2 + 1$ is odd, thus $2 \nmid m_1 + m_2 + 1$.

When $n = p$ is an odd prime number, $(1, p-2)$, $(2, p-3)$, ..., $((p-1)/2 - 1, (p-1)/2 + 1)$ are pairs of $(m_1, m_2)$ where $C(m_1) = C(m_2)$. And children corresponding to those $C(m)$ can get 2 gumballs in one period. The child with number $C((p-1)/2) \equiv \frac{p^2-9}{8} \pmod p$ will get 1 gumball in a period.

When $n = p^e$ for some odd prime $p$, let $f(m) = m^2 + m - 2 - 2C(m_0)$ for some $0 < m_0 \leqslant n$. For those $m_0$ where $f'(m_0) \not\equiv 0 \pmod p$, there are 2 solutions to $m^2 + m - 2 - 2C(m_0) \equiv 0 \pmod n$. For those $m_0$ where $f'(m_0) = 2m + 1 \equiv 0 \pmod p$, suppose $p^k | f(m_0)$ and $p^{k+1} \nmid f(m_0)$. By Hensel's lemma, there are $2p^{k-1}$ solutions if $C(m_0) \neq C((n-1)/2)$, and there are $p^{k-1}$ solutions otherwise.

When $n = 2^e$, the period of $C(m)$ is $2n$. Child $C(m)$ will also receive the gumball $2n - m - 1$ if $m < 2n - 1$. The $(n-1)$th child will receive $(2n-1)$th and $(2n)$th gumballs.

When $n = 2^{e_0} p_1^{e_1} \cdots p_k^{e_k}$, consider $\alpha \equiv \pmod{p_i^{e_i}}$ respectively and use Chinese Remainder Theorem to calculate the number of gumballs.