Math 4400 Homework 8
Due: Friday, July 28th, 2017

Feel free to work with your classmates, but everyone must turn in their own assignment. Please make a note of who you worked with on each problem. Let me know if you find a typo, or you're stuck on any of the problems.

1. Answer the following:
   (a) (5 points) Is 123 a square modulo 137?

Solution: We use quadratic reciprocity a bunch of times: first we factor $123 = 3 \cdot 41$. Then we compute:

$$\begin{aligned}\left(\frac{123}{137}\right) &= \left(\frac{3}{137}\right)\cdot\left(\frac{41}{137}\right) = \left(\frac{137}{3}\right)\cdot\left(\frac{137}{41}\right)\\ &= \left(\frac{2}{3}\right)\cdot\left(\frac{14}{41}\right) = -1\cdot\left(\frac{2}{41}\right)\cdot\left(\frac{7}{41}\right)\\ &= -1\cdot\left(\frac{2}{41}\right)\cdot\left(\frac{41}{7}\right) = -1\cdot\left(\frac{2}{41}\right)\cdot\left(\frac{-1}{7}\right)\end{aligned}$$

Further, we know $\left(\frac{2}{41}\right) = 1$ since $41 \equiv 1 \mod 8$ and $\left(\frac{-1}{7}\right) = -1$ since $7 \equiv 3 \mod 4$. So at the end of the day,

$$\left(\frac{123}{137}\right) = 1$$

which means 123 is, in fact, a square mod 137.

   (b) (5 points) Is 168 a square modulo 179?

Solution: First, we factor 168: $168 = 2^3 \cdot 3 \cdot 7$. Thus:

$$\left(\frac{168}{179}\right) = \left(\frac{2}{179}\right)^3 \cdot \left(\frac{3}{179}\right)\left(\frac{7}{179}\right)$$

Note: $179 \equiv 3 \mod 8$ and $179 \equiv 3 \mod 4$. Thus:

$$\begin{aligned}\left(\frac{2}{179}\right)^3 \cdot \left(\frac{3}{179}\right)\left(\frac{7}{179}\right) &= (-1)^3 \cdot (-1)\left(\frac{179}{3}\right)\cdot(-1)\left(\frac{179}{7}\right)\\ &= -\left(\frac{2}{3}\right)\cdot\left(\frac{4}{7}\right) = \left(\frac{2}{7}\right)^2 = 1\end{aligned}$$

Note that we don't have to actually compute $\left(\frac{2}{7}\right)$; whatever it is, its square is 1. Better yet, we could have argued that since $4 = 2^2$, that means $4 \equiv 2^2 \mod 7$, and so $\left(\frac{4}{7}\right) = 1$. So we see that 168 is a square modulo 179.

   (c) (5 points) Is 8 a square modulo 73?

Solution:

$$\left(\frac{8}{73}\right) = \left(\frac{2}{73}\right)^3 = 1$$

since $73 \equiv 1 \mod 8$

2. (5 points) Prove that an integer of the form $n^5 - n + 3, n \in \mathbb{Z}$ is never a square number (Hint: reduce modulo 5)

Solution: By Fermat's little theorem, $n^5 - n \equiv 0 \mod 5$ for all n. Thus, $n^5 - n + 3 \equiv 3 \mod 5$. But 3 isn't a square mod 5 which means $n^5 - n + 3$ can't be a square. Indeed, suppose $n^5 - n + 3 = a^2$ for some $a \in \mathbb{Z}$. Then we have $3 \equiv a^2 \mod 5$, a contradiction.

3. (10 points) Prove that $(\mathbb{Z}/p\mathbb{Z})^\times$ has an element of order 4 if and only if $p \equiv 1 \mod 4$.

Solution: (p is supposed to be an odd prime, as usual) Suppose $p \equiv 1 \mod 4$. Then there is some $a \in \mathbb{Z}$ such that $a^2 \equiv -1 \mod p$. This means that $a^4 = 1$ and a is an element of order 4 in $(\mathbb{Z}/p\mathbb{Z})^\times$. Indeed, if $a^4 = 1$, then a must be a primitive dth root for some d that divides 4. But a is not a 1st root or 2nd root of unity, so a must be a primitive 4th root of unity in $\mathbb{Z}/p\mathbb{Z}$ (which is the same thing as saying a has order 4 in $(\mathbb{Z}/p\mathbb{Z})^\times$).

For the other direction, suppose $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ is an element of order 4. That means $(g^2)^2 \equiv 1$, so $g^2 \equiv \pm 1$. But g is a primitive 4th root, which means $g^2 \not\equiv 1$. Thus $g^2 \equiv -1$. Thus -1 is a square mod p, which means $p \equiv 1 \mod 4$.

4. (10 points) Let p be an odd prime. In class, we learned that 2 is a square modulo p if and only if $p \equiv 1$ or $p \equiv 7 \mod 8$. Use quadratic reciprocity to find a similar law for determining when 3 is a square modulo p. In other words, find a number n such that the value of $\left(\frac{3}{p}\right)$ depends only on the equivalence class of p modulo n. For which equivalence classes is 3 a square modulo p? (Hint: your notes from our lecture on the chinese remainder theorem might be helpful, here)

Solution: (We should also assume that $p \neq 3$) By quadratic reciprocity,

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right), & p \equiv 1 \mod 4 \\ -\left(\frac{p}{3}\right), & p \equiv 3 \mod 4 \end{cases}$$

Thus 3 is a square mod p if and only if either:

- p is a square mod 3 and $p \equiv 1 \mod 4$, or
- p is not a square mod 3 and $p \equiv 3 \mod 4$

Now, since $p \neq 3$, $p \neq 0 \mod 3$. Thus $p \equiv 1 \mod 3$ if p is a square mod 3 and $p \equiv 2 \mod 3$ otherwise. So 3 is a square mod p if and only if

- $p \equiv 1 \mod 3$ and $p \equiv 1 \mod 4$, or

- $p \equiv 2 \mod 3$ and $p \equiv 3 \mod 4$

By the Chinese Remainder Theorem, there is some unique* $x \in \mathbb{Z}/12\mathbb{Z}$ such that $x \equiv 1 \mod 3$ and $x \equiv 1 \mod 4$. Clearly this x must be 1. Similarly, there is some unique $y \in \mathbb{Z}/12\mathbb{Z}$ such that $y \equiv 2 \mod 3$ and $y \equiv 3 \mod 4$. This y is 11. So we see that 3 is a square mod p if and only if $p \equiv 1$ or $11 \mod 12$.

*__Aside:__ Ok, so in class way back when, we showed that, if $m, n \in \mathbb{Z}$ are relatively prime, then for all $a, b \in \mathbb{Z}$ there exists a unique $x \in \{0, 1, \ldots, mn-1\}$ such that $x \equiv a \mod m$ and $x \equiv b \mod n$. But from this we can show that there's a unique $[y]_{mn} \in \mathbb{Z}/mn\mathbb{Z}$ satisfying $y \equiv a \mod m$ and $y \equiv b \mod n$. Indeed, from the above statement, we know that at least one such $[y]_{mn}$ exists: take $y = x$. For uniqueness, it's enough to show that if z is an integer with $z \equiv a \mod m$ and $z \equiv b \mod n$, then $z \equiv x \mod mn$, for then $[z]_{mn} = [x]_{mn}$. For this, note that, for all $c, d \in \mathbb{Z}$, if $c \equiv d \mod mn$ then $c \equiv d \mod m$ and $c \equiv d \mod n$. Further, we know there's some $w \in \{0, \ldots, mn-1\}$ with $w \equiv z \mod mn$. This means $w \equiv a \mod m$ and $x \equiv b \mod n$. But then $w = x$, so $z \equiv x \mod mn$, as desired.

5. (5 points) Let p be an odd prime. Suppose there exist $x, y \in \mathbb{Z}$ with $x^2 + y^2 = p$. Show that $p \equiv 1 \mod 4$. (In fact, the converse holds as well: if $p \equiv 1 \mod 4$, then there exist such x and y. Try some examples yourself!)

Solution: If $x^2 + y^2 = p$, then $x^2 \equiv -y^2 \mod p$. Note that we must have $0 < y < p$, so y is invertible mod p. Thus $(xy^{-1})^2 \equiv x^2 y^{-2} \equiv -1 \mod p$. But we know that -1 is a square mod p if and only if $p \equiv 1 \mod 4$, so this means $p \equiv 1 \mod 4$.

6. Suppose Alice's public key for RSA encryption is $(m = 703, e = 5)$.
   (a) (5 points) Encrypt the message 2017 to send to Alice.

Solution: We have some options, depending on how we want to break up the message into pieces smaller than m:

- $(2, 017)$ becomes $(2^5 \mod 703, 017^5 \mod 703) = (32, 500)$
- $(20, 17)$ becomes $(20^5 \mod 703, 17^5 \mod 703) = (647, 500)$
- $(201, 7)$ becomes $(201^5 \mod 703, 7^5 \mod 703) = (292, 638)$

   (b) (5 points) You're talking to someone who claims to be Alice, but you're suspicious! You ask this person to send a message to you signed by Alice's private key. The person writes back with the message, $12, 34$, followed by the signed message, $255, 231$. Verify that this person really is Alice.

Solution: We check:

$$255^5 \equiv 12 \mod 703,$$
$$231^5 \equiv 34 \mod 703,$$

as desired.

   (c) (5 points) Is $(m = 65, e = 10)$ a valid public key? Why or why not?

Solution: It's not valid: we must have e invertible modulo $\varphi(65)$. But $\varphi(65) = \varphi(5 \cdot 13) = 4 \cdot 12 = 48$, and $\gcd(10, 48) \neq 1$.

7. Your public key for RSA is $(m = 299, e = 5)$

   (a) (10 points) Find your private key, using the fact that $299 = 13 \cdot 23$.

Solution: We must find the inverse of e modulo $\varphi(m) = 12 \cdot 22 = 264$. We use the Euclidean algorithm:

$$264 = 52 \cdot 5 + 4$$
$$5 = 4 + 1$$

Thus,

$$5 - 4 = 1$$
$$5 - (264 - 52 \cdot 5) = 1$$
$$53 \cdot 5 - 264 = 1$$

Thus, our private key is $(m = 299, d = 53)$.

   (b) (5 points) Someone sends you the message $(169, 129)$. Decrypt this message using your private key.

Solution: We compute:

$$169^{53} \equiv 78 \mod 299$$
$$129^{53} \equiv 90 \mod 299$$

8. You're Varis and you're intercepting communications between Catelyn Stark and Brianne of Tarth. Here's a transcript of what you're able to read:

```
Catelyn: Let's use a Caesar cipher and do Diffie-Hellman to
         establish our secret key
Brianne: Sounds good
Catelyn: Ok, let's use p = 17 and g=10
Catelyn: X = 5
Brianne: Y = 11
Catelyn: ZHGGLQJ LV JRLQJ JUHDW
```

   (a) (10 points) Find either x or y. What is their shared secret?

Solution: To find x, we need to solve the equation $10^x \equiv X \mod 17$. The only method we know for doing this is to just try everything:

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$10^x \mod 17$	10	15	14	4	6	9	5	16	7	2	3	13	11	8	12	1

From the table, we see $x = 7$. Similarly, $y = 13$ since the table shows $10^{13} = Y$. The shared secret is $Y^x = X^y = 3 \mod 17$.

(b) (2 points) What does the message say?

Solution: Since the shared secret was 3, we have to shift all of the letters back by 3. The message becomes:
`WEDDING IS GOING GREAT`