Math 4400 Homework 7 Solutions key
Due: Monday, July 17th, 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. Solve the following equations:
   (a) (5 points) $x^{11} \equiv 13 \mod 35$

Solution: First, we check:

- $\gcd(13, 35) = 1$
- $\gcd(11, \varphi(35)) = \gcd(11, 24) = 1.$

This means we can apply proposition 19 to find the solution, applying it to the group $(\mathbb{Z}/35\mathbb{Z})^{\times}$: we start by computing the inverse of 11 modulo 24,

$$\begin{aligned} 24 &= 2 \cdot 11 + 2 \\ 11 &= 5 \cdot 2 + 1, \text{ so} \\ 1 &= 11 - 5 \cdot 2 = 11 - 5 \cdot (24 - 2 \cdot 11) = 11 \cdot 11 - 5 \cdot 24 \end{aligned}$$

We see that $11^{-1} \equiv 11 \mod 24$. So the answer is $x \equiv 13^{11} \mod 35$. To figure out this number, we proceed by repeated squaring,

$$\begin{aligned} 13^2 &\equiv 29 \\ 13^4 &\equiv 29^2 \equiv 1 \\ 13^8 &\equiv 1^2 \equiv 1 \end{aligned}$$

so $13^{11} \equiv 13^8 \cdot 13^2 \cdot 13 \equiv 1 \cdot 29 \cdot 13 \equiv 27$.

   (b) (5 points) $x^5 \equiv 3 \mod 64$

Solution: Similarly, we check:

- $\gcd(3, 64) \equiv 1$
- $\gcd(5, \varphi(64)) = \gcd(5, 32) = 1$

So we can use proposition 19. Next, we compute the inverse of 5 modulo 32. In this case it's not too hard to it in your head: $13 \cdot 5 \equiv 1 \mod 32$. So the solution is $x \equiv 3^{13}$. We compute,

$$\begin{aligned} 3^2 &\equiv 9 \mod 64 \\ 3^4 &\equiv 17 \mod 64 \\ 3^8 &\equiv 33 \mod 64 \end{aligned}$$

So $x \equiv 3^{13} \equiv 33 \cdot 17 \cdot 13 \equiv 61 \mod 64$

2. (10 points) Find all the 6^{th} roots of unity in $\mathbb{Z}/13\mathbb{Z}$. Which roots are primitive? (A calculator might be helpful, here).

Solution: We start by making a table of all the 6^{th} powers modulo 13:

x	1	2	3	4	5	6	7
$x^6 \mod 13$	1	12	1	1	12	12	12

Since 6 is even, we know $x^6 \equiv (-x)^6$ for all x, so the sixth roots of unity are $1, 3, 4, -1, -3$ and -4. To find the primitive sixth roots, we raise these numbers to the second and third powers:

x	1	3	4	-1	-3	-4
$x^2 \mod 13$	1	9	3	1	9	3

x	1	3	4	-1	-3	-4
$x^3 \mod 13$	1	1	12	-1	-1	-12

The first table shows $1, -1$ are not primitive, and the second table shows that 3 and -4 are not primitive. So the primitive sixth roots are 4 and -3, or equivalently 4 and 10.

3. (a) (5 points) Let p be a prime. Show that $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + 1$.

Solution: This is a quick application of our recursive formula for $\Phi_n(X)$:

$$\begin{aligned}\Phi_p(X) &= \frac{x^p - 1}{\prod_{d|p, d<p} \Phi_d(X)} = \frac{x^p - 1}{\Phi_1(X)} \\ &= \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1\end{aligned}$$

(b) (5 points) Compute $\Phi_8(X)$ and $\Phi_9(X)$.

Solution: For this, it's easiest to use the recursion formula,

$$\Phi_n(X) = \frac{X^n - 1}{\prod_{d|n, d<n} \Phi_d(X)}$$

In particular,

$$\Phi_8(X) = \frac{X^8 - 1}{\Phi_1(X)\Phi_2(X)\Phi_4(X)} = \frac{X^8 - 1}{(X-1)(X+1)(X^2+1)} = \frac{X^8 - 1}{(X^2-1)(X^2+1)} = \frac{X^8 - 1}{X^4 - 1}$$

using the values of Φ_1, Φ_2, and Φ_4 that we found in class. By the difference of squares formula, we see that $X^8 - 1$ factors as

$$X^8 - 1 = \left(X^4 + 1\right)\left(X^4 - 1\right)$$

so $\Phi_8(X) = X^4 + 1$
Similarly,

$$\Phi_9(X) = \frac{X^9 - 1}{\Phi_1(X)\Phi_3(X)} = \frac{X^9 - 1}{(X-1)\left(X^2 + X + 1\right)} = \frac{X^9 - 1}{X^3 - 1}$$

Applying the factorization,

$$Y^n - 1 = (Y-1)(Y^{n-1} + Y^{n-2} + \cdots + 1)$$

to the case where $n = 3$ and $Y = X^3$, we see that $X^9 - 1 = (X^3 - 1)(X^6 + X^3 + 1)$. So $\Phi_9(X) = X^6 + X^3 + 1$.

(c) (2 points) Conjecture a formula for $\Phi_{p^n}(X)$, where p is prime and n is an integer.

Solution: There are many possible conjectures that fit the data from parts (a) and (b); in any case, the correct formula is

$$\Phi_{p^n}(X) = \left(X^{p^{n-1}}\right)^{p-1} + \left(X^{p^{n-1}}\right)^{p-2} + \cdots + X^{p^{n-1}} + 1$$

4. (5 points) Let p be a prime. Prove that $\mathbb{Z}/p\mathbb{Z}$ has a primitive $(p-1)^{\text{th}}$ root of unity.

Solution: Fermat's little theorem tells us that every element of $(\mathbb{Z}/p\mathbb{Z})^\times$ is a $(p-1)^{\text{th}}$ root of unity. So there are $p-1$ distinct $(p-1)^{\text{th}}$ roots of unity in this field. Proposition 20 tells us that there exist $\varphi(p-1)$ primitive roots. In particular, there is at least one.

5. Let p be a prime and α a primitive $(p-1)^{\text{th}}$ root of unity in $\mathbb{Z}/p\mathbb{Z}$.

(a) (10 points) Let $x \in (\mathbb{Z}/p\mathbb{Z})^\times$. Prove that x can be written as α^n for some unique n in $\{1, 2, \ldots, p-1\}$. This number n is usually denoted $I(x)$, and is called the *index* of x modulo p, with respect to α. It's also called the *discrete logarithm* of x modulo p, with respect to α.

Solution: As noted in the solution to problem 4, Fermat's Little Theorem tells us that each element of $(\mathbb{Z}/p\mathbb{Z})^\times$ is a $(p-1)^{\text{st}}$ root of unity. In other words, $(\mathbb{Z}/p\mathbb{Z})^\times = \mu_{p-1}(\mathbb{Z}/p\mathbb{Z})$. As we mentioned in class, if α is a primitive root, then $\alpha, \alpha^2, \ldots, \alpha^{p-1}$ are all distinct elements of $(\mathbb{Z}/p\mathbb{Z})^\times$. Now, since $\mu_{p-1}(\mathbb{Z}/p\mathbb{Z})$ is closed under multiplication, we know $\mu_{p-1}(\mathbb{Z}/p\mathbb{Z}) \supseteq \left\{\alpha^1, \ldots, \alpha^{p-1}\right\}$. But both sets have size $p-1$, so they must be equal. This finishes the proof: we've just shown that each element of $(\mathbb{Z}/p\mathbb{Z})^\times$ can be written as α^n for some n in $\{1, 2, \ldots, p-1\}$. Since $\alpha^1, \ldots, \alpha^{p-1}$ are all distinct, this n is unique.

For the sake of completeness, let's reprove that $\alpha, \alpha^2, \ldots, \alpha^{p-1}$ are all distinct. Well, if $\alpha^i = \alpha^j$ for some $i, j \in \{1, 2, \ldots, p-1\}$, then $\alpha^{i-j} = 1$. But $0 \leq i-j \leq p-2$. By definition of a primitive root, we must have $i-j = 0$, so $i = j$.

(b) (5 points) Show that the function $I : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}/(p-1)\mathbb{Z}$ is a homomorphism.

Solution: Note: if $a \equiv b \mod (p-1)$, then $\alpha^a = \alpha^b$. So $I(\alpha^a) = [a]_{p-1}$ for all $a \in \mathbb{Z}$, and not just for all $a \in \{1, 2, \ldots, p-1\}$. Thus:

$$I(\alpha^i \alpha^j) = I(\alpha^{i+j}) = [i+j] = [i] + [j] = I(\alpha^i) + I(\alpha^j)$$

as desired.

6. (10 points) Let $n > 1$ be an integer. Show that $\displaystyle\sum_{\zeta \in \mu_n(\mathbb{C})} \zeta = 0$. (Hint: what happens when you multiply that sum by any $\zeta \in \mu_n(\mathbb{C})$?)

Solution: Since $n > 1$, there exists some nth root of unity $\alpha \in \mu_n(\mathbb{C})$ such that $\alpha \neq 1$ (for instance, we can always take $\alpha = e^{2\pi i/n}$). Notice that

$$\alpha \cdot \sum_{\zeta \in \mu_n(\mathbb{C})} \zeta = \sum_{\zeta \in \mu_n(\mathbb{C})} \alpha \cdot \zeta$$

Also, if $\zeta \in \mu_n(\mathbb{C})$, then $\alpha\zeta \in \mu_n(\mathbb{C})$, since $\mu_n(\mathbb{C})$ is a group under multiplication. So

$$\{\alpha\zeta \mid \zeta \in \mu_n(\mathbb{C})\} \subseteq \mu_n(\mathbb{C}).$$

On the other hand, for all $\zeta \in \mu_n(\mathbb{C})$, $\alpha^{-1}\zeta \in \mu_n(\mathbb{C})$ and $\zeta = \alpha\left(\alpha^{-1}\zeta\right)$. This shows that each $\zeta \in \mu_n(\mathbb{C})$ is a term in the summation $\sum_{\zeta\in\mu_n(\mathbb{C})} \alpha \cdot \zeta$. Finally, each $\zeta \in \mu_n(\mathbb{C})$ appears in the summation $\sum_{\zeta\in\mu_n(\mathbb{C})} \alpha \cdot \zeta$ exactly once: if $\alpha\zeta_1 = \alpha\zeta_2$, then $\zeta_1 = \zeta_2$, since $\alpha \neq 0$. Thus,

$$\sum_{\zeta\in\mu_n(\mathbb{C})} \alpha \cdot \zeta = \sum_{\zeta\in\mu_n(\mathbb{C})} \zeta$$

Combining this with the first equation, we have

$$\alpha \cdot \sum_{\zeta\in\mu_n(\mathbb{C})} \zeta = \sum_{\zeta\in\mu_n(\mathbb{C})} \zeta$$

Now suppose that $\sum_{\zeta\in\mu_n(\mathbb{C})} \zeta \neq 0$. Then we can multiply each side of the above equation by $\left(\sum_{\zeta\in\mu_n(\mathbb{C})} \zeta\right)^{-1}$ to get $\alpha = 1$. But this is a contradiction.

7. (a) (10 points) Let p be an odd prime. Prove that exactly $(p-1)/2$ elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ are squares.

Solution: Let $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ be primitive. Then $(\mathbb{Z}/p\mathbb{Z})^\times = \left\{g^1, \dots, g^{p-1}\right\}$ by problem 5a. But we learned that g^n is a square if and only if n is even. Since 1 is odd and $p-1$ is even, exactly half the elements of $\{1, 2, \dots, p-1\}$ are even, which completes the proof.

(b) (5 points) Use part (a) to show that, for each odd prime p, there exists a field of order p^2.

Solution: By part (a), for each odd prime p there exists some integer $d \in \mathbb{Z}$ such that d is *not* a square modulo p. But this means that $\mathbb{Z}[\sqrt{d}]/p\mathbb{Z}[\sqrt{d}]$ is a field of size p^2.

8. (5 points) Use Euler's criterion to determine if the following are squares:

(a) 3 modulo 31

Solution: Euler's criterion tells us that we need to check what 3^{15} is congruent to modulo 31. We compute

$$\begin{aligned} 3 &\equiv 3 \\ 3^2 &\equiv 9 \\ 3^4 &\equiv 19 \\ 3^8 &\equiv 20 \end{aligned}$$

So $3^{15} \equiv 3^8 3^4 3^2 3^1 \equiv 20 \cdot 19 \cdot 9 \cdot 3 \equiv\equiv -1$. Thus, 3 is not a square modulo 31, by Euler's criterion.

(b) 7 modulo 29

Solution: Euler's criterion tells us that we need to check what 7^{14} is congruent to modulo 29. We compute

$$\begin{aligned} 7 &\equiv 7 \\ 7^2 &\equiv 20 \\ 7^4 &\equiv 23 \\ 7^8 &\equiv 7 \end{aligned}$$

So $7^{15} \equiv 7 \cdot 23 \cdot 20 \equiv 1$, so 7 is a square modulo 29, by Euler's criterion.

9. (5 points) Let n be a positive integer. Let p be a prime divisor of n^2+1. Prove that $p \equiv 1 \mod 4$ (Hint: use proposition 23).

Solution: (We also need to assume that $p \neq 2$ for this problem; oops!) If p is a divisor of n^2+1, then $n^2 \equiv -1 \mod p$. In other words, -1 is a square modulo p. Thus $p \equiv 1 \mod 4$ by proposition 23.

10. (10 points) Use the above to show that there are infinitely many primes congruent to 1 modulo 4. (Hint: come up with infinitely many numbers of the form n^2+1 that are all relatively prime to one-another).

Solution: Consider the sequence:

$$\begin{aligned} a_1 &= 5 \\ a_{n+1} &= \left(\prod_{i=1}^{n} a_n\right)^2 + 1 \end{aligned}$$

Each a_i must have an odd prime divisor p_i, since $a_i > 2$ for all i. By the previous problem, $p_i \equiv 1 \mod 4$. On the other hand, for all distinct $i, j \in \mathbb{Z}$, $j > i \geq 1$, a_i and a_j are relatively prime: that's because $a_j \equiv 1p$ for all primes p dividing a_i, so in particular a_j is not divisible by any primes dividing a_i. This tells us that $p_i \neq p_j$, so the set $\{p_i \mid i \geq 1\}$ is an infinite set of primes congruent to 1 modulo 4.