# Math 4400 Final Exam

August 4, 2017

Name: Solutions

You may assume, without proof:

- If $a, b \in \mathbb{N}$ and $ab = 1$, then $a = 1$ and $b = 1$
- If $a \mid b$ and $b \mid c$, then $a \mid c$
- If $ac \mid bc$ and $c \neq 0$, then $a \mid b$.

| Question | Points | Score |
|---|---|---|
| 1 | 10 | |
| 2 | 5 | |
| 3 | 5 | |
| 4 | 5 | |
| 5 | 5 | |
| 6 | 10 | |
| 7 | 5 | |
| 8 | 10 | |
| 9 | 5 | |
| 10 | 10 | |
| 11 | 5 | |
| 12 | 20 | |
| 13 | 5 | |
| 14 | 0 | |
| Total: | 100 | |

## Computations

1. (a) (5 points) Compute gcd(119, 448)

$448 = 3 \cdot 119 + 91$

$119 = 1 \cdot 91 + 28$

$91 = 3 \cdot 28 + 7$

$28 = 4 \cdot 7$

$\gcd = 7.$

(b) (5 points) Find the continued fraction expansion of $\frac{448}{119}$

$$\frac{448}{119} = [3; 1, 3, 4]$$

2. (5 points) Find all the incongruent solutions to $7x \equiv 15 \mod 100$

$100 = 14 \cdot 7 + 2, \quad 7 = 3 \cdot 2 + 1$

$\Rightarrow 7 - 3 \cdot 2 = 7 - 3 \cdot (100 - 14 \cdot 7) = 43 \cdot 7 - 3 \cdot 100 = 1$

$\Rightarrow 7^{-1} \equiv 43 \mod 100$

$\Rightarrow x \equiv 43 \cdot 15 = 45 \mod 100$

3. (5 points) Find $x$ with $0 \leq x < 253$ such that $15^{444} \equiv x \mod 253$. The prime factorization of 253 is $11 \cdot 23$. Here are the first few powers of 15 modulo 253:

$$15^2 \equiv 225, \quad 15^3 \equiv 86, \quad 15^4 \equiv 25, \quad 15^5 \equiv 122, \quad 15^6 \equiv 59$$

$\varphi(253) = 10 \cdot 22 = 220$

$444 \equiv 4 \mod 220, \quad 10$

$15^{444} \equiv 15^4 \equiv 25 \mod 253$

4. (5 points) Find all the incongruent solutions to: $x^{19} \equiv 16 \mod 19$

Fermat's little theorem implies $x^{19} \equiv x \mod 19$ $\forall x \in \mathbb{Z}$. Thus $x \equiv x^{19} \equiv 16 \mod 19$

$\Rightarrow x \equiv 16 \mod 19.$

5. (5 points) Compute the polynomial: $\dfrac{x^8 - 1}{\Phi_8(X)\Phi_4(X)}$

$$X^8 - 1 = \Phi_1(X) \cdot \Phi_2(X) \cdot \Phi_4(X) \cdot \Phi_8(X)$$

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

6. (10 points) $3x^5 + 17x - 6 \equiv 0 \mod 51$. (Hint: $51 = \cancel{7 \cdot 13}$ $17 \cdot 3$. Use the Chinese Remainder Theorem)

Work mod 3 and mod 17:

Mod 3: $17x \equiv 6 \mod 3 \Leftrightarrow x \equiv 0 \mod 3$.

Mod 17: $3x^5 \equiv 6 \equiv 2 \cdot 3 \mod 17$.

$\Leftrightarrow x^5 \equiv 2 \mod 17$ (since 3 is invertible mod 17)

$\gcd(5, \varphi(17)) = 1$, $\gcd(2, 17) = 1$

$\Rightarrow$ Find $5^{-1} \mod \varphi(17) = 16$:

$16 = 3 \cdot 5 + 1 \Rightarrow -3 \cdot 5 \equiv 1 \mod 16$

$\Rightarrow x \equiv 2^{-3} \equiv 2^{13} \equiv 15 \mod 17$

$\Rightarrow$ Solution is the unique $x \in \mathbb{Z}/51\mathbb{Z}$ with $x \equiv 0 \mod 3$ and $x \equiv 15 \mod 17$.

Clearly, $x \equiv 15 \mod 51$ works.

7. (5 points) Is 105 a square modulo 239? (239 is a prime number)

$$\left(\frac{105}{239}\right) = \left(\frac{5}{239}\right) \cdot \left(\frac{23}{239}\right) = \underbrace{\left(\frac{239}{5}\right)}_{5 \equiv 1 \bmod 4} \cdot (-1) \cdot \underbrace{\left(\frac{239}{23}\right)}_{239 \equiv 23 \equiv 3 \bmod 4}$$

$$= \underbrace{\left(\frac{4}{5}\right)}_{=1 \text{ since } 4 \text{ is a square}} \cdot (-1) \cdot \underbrace{\left(\frac{9}{23}\right)}_{=1 \text{ since } 9 \text{ is a square}}$$

$$= -1$$

No, it's not a square mod 239

8. (10 points) Give an example of a public/private key pair for $RSA$ using $m = 11 \cdot 23 = 253$. Make sure to explain your reasoning!

We just need $\gcd(e, \varphi(253)) = 1$

and $d \cdot e \equiv 1 \mod \varphi(253)$

$\varphi(253) = 10 \cdot 22 = 220$

E.g. Choose $e = 3$. Then

$220 = 73 \cdot 3 + 1$

$\Rightarrow -73 \cdot 3 \equiv 1 \mod 220$

$d \equiv -73 \equiv 147 \mod 220$

$\Rightarrow (253, 3), (253, 147)$ works.

## Proofs

9. (5 points) Suppose $\gcd(a, b) = 1$, $a \mid bc$. Show $a \mid c$.

$\exists\, x, y \in \mathbb{Z}$ s.t. $ax + by = 1$, by Bezout.

$\Rightarrow \quad axc + byc = c$

$a \mid axc$, $\quad a \mid byc$ (since $a \mid bc$)

$\Rightarrow \quad a \mid axc + byc = c$.

10. (10 points) Suppose $a, b, c \in \mathbb{Z}$ with $\gcd(a, \gcd(b, c)) = 1$. Show there exist $x, y, z \in \mathbb{Z}$ such that $ax + by + cz = 1$.

By Bezout, $\exists\, d, e \in \mathbb{Z}$ s.t.

$$ad + \gcd(b,c) \cdot e = 1$$

By Bezout, $\exists\, f, g \in \mathbb{Z}$ s.t. $bf + cg = \gcd(b,c)$

$$\Longrightarrow ad + bfe + cge = 1$$

Choose $x = d$, $y = fe$, $z = ge$.

$|G| = \#G$
(alternate notation)

11. (5 points) Let $p$ be a prime number. Prove that any group of order $p$ is cyclic.

Let $|G| = p$. Then $|G| > 1$, so $\exists g \in G$ with $g \neq e$.

Thus, $\#\langle g \rangle > 1$. By Lagrange, $\#\langle g \rangle \mid |G|$

$\Rightarrow \#\langle g \rangle = p$, so $G = \langle g \rangle$

12. Let $F$ be a field, $n > 1$, and $g$ a primitive $n^{\text{th}}$ root of unity in $F$.

(a) (5 points) Suppose $g^m = 1$ for some $m \in \mathbb{Z}$. Prove that $n \mid m$.

Division algo: $\exists q, r$: $m = qn + r$ with $0 \leq r < n$

$\Rightarrow 1 = g^m = (g^n)^q \cdot g^r = 1^q \cdot g^r = g^r$

Since $0 \leq r < n$ and $g$ is a primitive $n^{th}$ root, we have $r = 0$

$\Rightarrow n \mid m$.

(b) (5 points) Let $i, j \in \mathbb{Z}$. Prove that $g^i = g^j$ if and only if $i \equiv j \mod n$.

If $g^i = g^j$, then $g^{i-j} = 1$ (since $g \neq 0$)

Part a) $\Rightarrow$ $n \mid i-j$, so $i \equiv j \mod n$

If $i \equiv j \mod n$, $\exists k \in \mathbb{Z}$: $i = kn + j$

$\Rightarrow g^i = g^{kn+j} = (g^n)^k \cdot g^j = g^j$.

(c) (10 points) Suppose that $d \in \mathbb{Z}$ and suppose that $g^d$ is also a primitive $n^{\text{th}}$ root of unity. Prove that $\gcd(d, n) = 1$.

By (b), $(g^d)^e = 1 \Leftrightarrow de \equiv 0 \mod n$

~~Thus~~ Note, $(g^d)^n = (g^n)^d = 1$.

Thus, $g^d$ primitive $\Rightarrow (g^d)^e \neq 1$ for $0 < e < n$

$\Rightarrow de \not\equiv 0 \mod n$, for $0 < e < n$

$\Rightarrow o(d) = n$ in $\mathbb{Z}/n\mathbb{Z}$

$\Rightarrow \frac{n}{\gcd(d,n)} = n$

$\Rightarrow \gcd(d,n) = 1$.

13. (5 points) Let $p$ be an odd prime and let $A \in \mathbb{Z}$. Suppose $p \mid A^2 - 5$. Show that $p \equiv 1$ or 4 mod 5.

$$p \mid A^2 - 5 \Rightarrow A^2 \equiv 5 \bmod p \Rightarrow \left(\frac{5}{p}\right) = 1$$

$$\Rightarrow \left(\frac{p}{5}\right) = 1.$$

| $x$ | 1 | 2 | 3 | 4 |
| --- | --- | --- | --- | --- |
| $x^2$ mod 5 | 1 | 4 | 4 | 1 |

$$\Rightarrow p \equiv 1 \text{ or } 4 \bmod 5$$

14. 5 pts ~~(10 points (bonus))~~ Let $n \in \mathbb{Z}$ and let $p$ be a prime not dividing $n$. Show there exists ~~some $N$ such that $n$~~ $e$ s.t. $n \mid (p^e - 1)$ ~~for all integers $e \geq N$~~.

Pf: