Math 255: Spring 2018
Practice Final Exam

NAME: SOLUTIONS

Time: **2 hours and 45 minutes**

For each problem, you **must** write down all of your work carefully and legibly to receive full credit. For each question, you **must** use theorems and/or mathematical reasoning to support your answer, as appropriate.

Failure to follow these instructions will constitute a breach of the UVM Code of Academic Integrity:

- You may not use a calculator or any notes or book during the exam.
- You may not access your cell phone during the exam for any reason; if you think that you will want to check the time please wear a watch.
- The work you present must be your own.
- Finally, you will more generally be bound by the UVM Code of Academic Integrity, which stipulates among other things that you may not communicate with anyone other than the instructor during the exam, or look at anyone else's solutions.

I understand and accept these instructions.

Signature: ______________________________

Problem	Value	Score
1	4	
2	5	
3	8	
4	12	
5	8	
6	15	
7	8	
8	8	
9	8	
10	8	
11	8	
12	8	
GC	8	
TOTAL	100 (or 108)	

Problem 1 : (4 points) Compute $8^{-1} \pmod{29}$.

$29 = 3\cdot 8 + 5$

$8 = 5 + 3$

$5 = 3 + 2$

$3 = 2 + 1$

$1 = 3 - 2$

$= 3 - (5-3) = 2\cdot 3 - 5$

$= 2(8-5) - 5 = 2\cdot 8 - 3\cdot 5$

$= 2\cdot 8 - 3(29 - 3\cdot 8)$

$= 11\cdot 8 - 3\cdot 29$

So $8^{-1} \equiv 11 \pmod{29}$

Problem 2 : (5 points) What is the (multiplicative) order of 2 modulo 11?

Since $\varphi(11) = 11 - 1 = 10$, the order of 2 divides 10, so it can be 1, 2, 5 or 10.

$2^1 \equiv 2 \not\equiv 1 \pmod{11}$

$2^2 \equiv 4 \not\equiv 1 \pmod{11}$

$2^5 \equiv 2^4\cdot 2 \equiv 16\cdot 2 \equiv 5\cdot 2 \equiv 10 \not\equiv 1 \pmod{11}$

We know $2^{10} \equiv 1 \bmod 11$ by Euler's Theorem (or Fermat's since 11 is prime). So the order of 2 modulo 11 is 10. Bonus: 2 is a primitive root of 11.

Problem 3 : (8 points) Give all **positive** integer solutions to the equation $39x + 51y = 3$.

$51 = 39 + 12$

$39 = 3\cdot 12 + 3$

$12 = 4\cdot 3$

$$\begin{aligned} 3 &= 39 - 3\cdot 12 \\ &= 39 - 3(51 - 39) \\ &= 4\cdot 39 - 3\cdot 51 \end{aligned}$$

$(39,51)=3$ and $3|3$ so there are integer solutions to this equation

A particular solution is $x_p = 4$, $y_p = -3$

The formula is $x = x_p + \frac{b}{(a,b)}t = 4 + 17t$ $\quad t \in \mathbb{Z}$

$y = y_p - \frac{a}{(a,b)}t = -3 - 13t$

Now we find what t's give positive x & y:

$x = 4 + 17t > 0$

$17t > -4$

$t > \frac{-4}{17}$

$t \geq 0$ since $t \in \mathbb{Z}$

$y = -3 - 13t > 0$

$-3 > 13t$

$\frac{-3}{13} > t$

$t \leq -1$ since $t \in \mathbb{Z}$

There are no values of t that satisfy both these constraints so there are no positive integer solutions to this equation

Problem 4 : (12 points) Solve the following equations. For each equation, give **all** distinct solutions (if there are more than one) and be sure to clearly indicate which ring the solutions belong to.

a) $4x \equiv 5 \pmod 6$

We have $(4,6)=2$ but $2 \nmid 5$ so there are no solutions to this congruence.

b) $13x \equiv 1 \pmod{17}$

$(13,17)=1$ so there is a unique solution

$17 = 13 + 4$

$13 = 3 \cdot 4 + 1$

$1 = 13 - 3 \cdot 4$

$= 13 - 3(17-13) = 4 \cdot 13 - 3 \cdot 17$

So $\boxed{x \equiv 13^{-1} \equiv 4 \pmod{17}}$

c) $15x \equiv 10 \pmod{25}$

$(15,25)=5$ and $5 \mid 10$ so there will be solutions

Divide through: $3x \equiv 2 \pmod 5$

$6x \equiv 4 \pmod 5$

$\boxed{x \equiv 4 \pmod 5}$

OR $\boxed{x \equiv 4, 9, 14, 19, 24 \pmod{25}}$

Problem 5 : (8 points) Solve the following systems of equations. Be sure to give **all** distinct solutions (if there are more than one) and to clearly indicate which ring the solution(s) belong to.

a) $x \equiv 1 \pmod{2}$, $3x \equiv 1 \pmod{5}$, $4x \equiv 5 \pmod{7}$

The moduli are coprime so we can do CRT directly

$M_1 = 35 \quad x_1 \equiv 35^{-1} \equiv 1^{-1} \equiv 1 \pmod{2}$

$M_2 = 14 \quad x_2 \equiv 14^{-1} \equiv 4^{-1} \equiv -1 \pmod{5}$

$M_3 = 10 \quad x_3 \equiv 10^{-1} \equiv 3^{-1} \equiv (-4)^{-1} \equiv -2 \pmod{7}$

Don't forget to put the equations in the correct form! $x \equiv 1 \pmod{2}$ $x \equiv 2 \pmod{5}$ $x \equiv 10 \equiv 3 \pmod{7}$

$$x \equiv 1 \cdot 35 \cdot 1 - 2 \cdot 14 \cdot 1 - 3 \cdot 10 \cdot 2 \pmod{70}$$

$$\equiv 35 - 28 - 60 \equiv 35 - 28 + 10 \equiv 17 \pmod{70}$$

$$\boxed{x \equiv 17 \pmod{70}}$$

b) $2x \equiv 4 \pmod{24}$, $3x \equiv 8 \pmod{10}$, $2x \equiv 22 \pmod{45}$

The moduli are not coprime, so first we solve each equation:

$x \equiv 2 \pmod{12}$ $\quad x \equiv 6 \pmod{10}$ $\quad x \equiv 11 \pmod{45}$

Split into prime factors:

$x \equiv 2 \pmod{3}$ $\quad x \equiv 6 \equiv 0 \pmod{2}$ $\quad x \equiv 11 \equiv 1 \pmod{5}$

$x \equiv 2 \pmod{4}$ $\quad x \equiv 6 \equiv 1 \pmod{5}$ $\quad x \equiv 11 \equiv 2 \pmod{9}$

Keep: $x \equiv 2 \pmod{4}$ $\quad x \equiv 2 \pmod{9}$ $\quad x \equiv 1 \pmod{5}$

$M_1 = 45 \quad x_1 \equiv 45^{-1} \equiv 1^{-1} \equiv 1 \pmod{4}$

$M_2 = 20 \quad x_2 \equiv 20^{-1} \equiv 2^{-1} \equiv 5 \pmod{9}$

$M_3 = 36 \quad x_3 \equiv 36^{-1} \equiv 1^{-1} \equiv 1 \pmod{5}$

$$x \equiv 2 \cdot 45 \cdot 1 + 2 \cdot 20 \cdot 5 + 1 \cdot 36 \cdot 1 \equiv 90 + 200 + 36 \pmod{180}$$

$$\equiv 90 + 20 + 36 \pmod{180}$$

$$\boxed{x \equiv 146 \pmod{180}}$$

Problem 6 : (15 points) Give all solutions to the following quadratic congruences.

a) $x^2 \equiv 65 \pmod{128}$ $\qquad 128 = 2\cdot 64 = 2^2\cdot 32 = 2^3\cdot 16 = 2^4\cdot 8 = 2^7$

First solve $x^2 \equiv 65 \equiv 1 \pmod{8}$. This has solution $x \equiv 1 \pmod{8}$

Next solve $x^2 \equiv 65 \equiv 1 \pmod{16}$. This has solution $x \equiv 1 \pmod{16}$

(or we could lift, but if we see the solution we don't have to)

Next solve $x^2 \equiv 65 \equiv 1 \pmod{32}$. This has solution $x \equiv 1 \pmod{32}$

Next solve $x^2 \equiv 65 \equiv 1 \pmod{64}$. This has solution

$x \equiv 1 \pmod{64}$

Finally solve $x^2 \equiv 65 \pmod{128}$ by lifting.

$x_1 = 1 + 32 y_0$ (lifting equation, with "step back" since $p=2$)

$$(1+32y_0)^2 \equiv 65 \pmod{128}$$

$$1 + 64y_0 + 32^2 y_0^2 \equiv 65 \pmod{128}$$

$$64 y_0 \equiv 64 \pmod{128}$$

$$y_0 \equiv 1 \pmod{2} \quad \rightarrow \quad x \equiv 1 + 32 \equiv 33 \pmod{128}$$

Since $p=2$, there are 4 solutions:

$x \equiv 33 \pmod{128}$ $\qquad x \equiv 33 + 64 \equiv 97 \pmod{128}$

$x \equiv -33 \equiv 95 \pmod{128}$ $\qquad x \equiv -97 \equiv 31 \pmod{128}$

$$\boxed{x \equiv 31, 33, 95, 97 \pmod{128}}$$

b) $x^2 \equiv 23 \pmod{121}$ $121 = 11^2$

First we solve $x^2 \equiv 23 \equiv 1 \pmod{11}$. This has solution $x \equiv 1 \pmod{11}$.

Next we lift!

$$x_1 = 1 + 11y_0$$

$$(1+11y_0)^2 \equiv 23 \pmod{121}$$

$$1 + 22y_0 + 121y_0^2 \equiv 23 \pmod{121}$$

$$22y_0 \equiv 22 \pmod{121}$$

$$y_0 \equiv 1 \pmod{11}$$

So $x \equiv 1 + 11 \equiv 12 \pmod{121}$

Since $p=11$ is odd, this has 2 solutions:

$x \equiv 12 \pmod{121}$

$x \equiv -12 \equiv 109 \pmod{121}$

$$\boxed{x \equiv 12, 109 \pmod{121}}$$

c) $x^2 \equiv 9 \pmod{20}$ $20 = 4 \cdot 5$

So we solve separately $x^2 \equiv 9 \equiv 1 \pmod 4$, which has solutions $x \equiv 1, 3 \pmod 4$

and $x^2 \equiv 9 \equiv 4 \pmod 5$ which has solutions $x \equiv 2, 3 \pmod 5$.

Next we get the four solutions modulo 20:

$M_1 = 5 \quad x_1 \equiv 5^{-1} \equiv 1^{-1} \equiv 1 \pmod 4$

$M_2 = 4 \quad x_2 \equiv 4^{-1} \equiv (-1)^{-1} \equiv -1 \pmod 5$

So the solutions will be $x \equiv 5a_1 - 4a_2 \pmod{20}$

$a_1 = 1, a_2 = 2$: $x \equiv 5 - 8 \equiv -3 \equiv 17 \pmod{20}$

$a_1 = 1, a_2 = 3$: $x \equiv 5 - 12 \equiv -7 \equiv 13 \pmod{20}$

$a_1 = 3, a_2 = 2$: $x \equiv 15 - 8 \equiv 7 \pmod{20}$

$a_1 = 3, a_2 = 3$: $x \equiv 15 - 12 \equiv 3 \pmod{20}$

$$\boxed{x \equiv 3, 7, 13, 17 \pmod{20}}$$

Problem 7 : (8 points) Let a be an integer. Show that a and a^{4n+1} always have the same last digit. i.e. show $a^{4n+1} \equiv a \pmod{10}$

- If $(a,10)=1$, we can apply Euler's Theorem: Since $\varphi(10) = 10(1-\frac{1}{2})(1-\frac{1}{5}) = 10 \cdot \frac{1}{2} \cdot \frac{4}{5} = 4$, we have

$$a^{4n+1} \equiv (a^4)^n \cdot a \equiv 1^n \cdot a \equiv a \pmod{10}$$

- If $(a,10)=2$; then $a \equiv 0 \pmod 2$ so $a^{4n+1} \equiv 0^{4n+1} \equiv 0 \pmod 2$ and $a^{4n+1} \equiv a \pmod 2$. Also, $(a,5)=1$, so by Fermat's Theorem, $a^4 \equiv 1 \pmod 5$ so $a^{4n+1} \equiv (a^4)^n \cdot a \equiv 1^n \cdot a \equiv a \pmod 5$. Since $a^{4n+1} \equiv a \pmod 2$ and $a^{4n+1} \equiv a \pmod 5$, by the Chinese Remainder Theorem $a^{4n+1} \equiv a \pmod{10}$

- If $(a,10)=5$, then $a \equiv 0 \pmod 5$ and so $a^{4n+1} \equiv 0 \equiv a \pmod 5$ Also $(a,2)=1$ so $a \equiv 1 \pmod 2$ and $a^{4n+1} \equiv 1 \equiv a \pmod 2$ Again since $a^{4n+1} \equiv a \pmod 2$ and $a^{4n+1} \equiv a \pmod 5$, then $a^{4n+1} \equiv a \pmod{10}$

- Finally if $(a,10)=10$, then $a \equiv 0 \pmod{10}$ so $a^{4n+1} \equiv 0 \equiv a \pmod{10}$

Since the only positive divisors of 10 are 1, 2, 5, 10, a must be in one of those four cases, so in any case $a^{4n+1} \equiv a \pmod{10}$.

Problem 8 : (8 points) In 1644, Mersenne asked for a positive integer with 60 distinct divisors. Find one such integer that is smaller than 10,000.

If $n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$ is n's prime-power factorization, then

$$d(n)=(e_1+1)(e_2+1)\cdots(e_k+1)$$

is the number of distinct divisors.

So we have looking for some $e_1, e_2, \ldots, e_k$ with

$$(e_1+1)(e_2+1)\cdots(e_k+1)=60$$

but also n is not too big. This can be done by picking the e_i's to be as small as possible, and then the p_i's to be small too.

We have $60=2\cdot 30=2\cdot 2\cdot 15=2\cdot 2\cdot 3\cdot 5$

so we can pick
$$\begin{aligned} e_1+1&=2 \to e_1=1\\ e_2+1&=2 \to e_2=1\\ e_3+1&=3 \to e_3=2\\ e_4+1&=5 \to e_4=4 \end{aligned}$$

$n=p_1p_2p_3^2p_4^4$ will have 60 distinct divisors if $p_i\neq p_j$

Now to keep n small pick $p_4=2$, $p_3=3$, $p_2=5$, $p_1=7$ so

$$n=2^4\cdot 3^2\cdot 5\cdot 7=16\cdot 9\cdot 35=144\cdot 35 < 200\cdot 50=10{,}000$$

$(n=5040)$

Problem 9 : (8 points) Let n be a positive integer with $6|n$. Show that $\phi(n) \leq \frac{n}{3}$.

We have that $n = 2^{f_1} 3^{f_2} p_1^{e_1} \cdots p_k^{e_k}$

with $f_1 \geq 1$, $f_2 \geq 1$ (since $6|n$)

and the p_i's are primes ≥ 5, $e_k \geq 1$

(possibly $k=0$ if no other primes divide n)

Then $$\varphi(n) = n \underset{\uparrow}{\left(1-\frac{1}{2}\right)}\underset{\uparrow}{\left(1-\frac{1}{3}\right)} \prod_{i=1}^{k} \underset{\uparrow}{\left(1-\frac{1}{p_i}\right)}$$

definitely there since $6|n$

other primes

$$= n \cdot \frac{1}{2} \cdot \frac{2}{3} \prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$$

$$= \frac{n}{3} \cdot \prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$$

Now if $k=0$, then $\varphi(n) = \frac{n}{3}$ and we are done

Otherwise, we have that each factor $1-\frac{1}{p_i} = \frac{p_i-1}{p_i} < 1$

So the product $\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right) < 1$. Therefore $\varphi(n) < \frac{n}{3}$

in that case, and the claim is proved.

Problem 10 : (8 points) Let $a > 1$ and $m > 1$ be integers, and let p be a prime. Show that if $p \equiv a \pmod{m}$, then $(a, m) = 1$ or $a = p$.

If $p \equiv a \pmod{m}$, then there is an integer k with

$$p = a + km.$$

Now let $d = (a, m)$. Then

$$p = d\left(\frac{a}{d} + k\frac{m}{d}\right)$$

and both $\frac{a}{d}$ and $\frac{m}{d}$ are integers. Since p is a prime, its only positive divisors are 1 and p. Since $d > 0$, either $d = 1$, in which case we are done since $d = (a, m) = 1$, or $d = p$.

If $d = p$, then $\frac{a}{d} + k\frac{m}{d} = \frac{a}{p} + k\frac{m}{p} = 1$.

we have that $a, p, m > 0$, so $\frac{a}{p}$ and $\frac{m}{p}$ are positive integers. Therefore $\frac{a}{p} + k\frac{m}{p} = 1$ is only possible if $k = 0$, so $\frac{a}{p} = 1$ or $a = p$.

Problem 11 : (8 points) Let p be a prime. Prove that

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

Note: You can use this fact on the Final Exam. It is sometimes called the Freshman's Dream, for reasons you can perhaps imagine.

By the Binomial Theorem,

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}$$

where $\binom{p}{i} = \frac{p!}{i!(p-i)!}$. If $0 < i < p$, then $0 < p-i < p$ also, and therefore p does not divide $i!$ or $(p-i)!$. Therefore p divides $\frac{p!}{i!(p-i)!} = \binom{p}{i}$, and

all terms in the middle are 0 modulo p. ↙

$$(a+b)^p \equiv \binom{p}{0} a^0 b^p + \binom{p}{p} a^p b^{p-p} \pmod{p}$$

$$\equiv b^p + a^p \pmod{p}$$

$$\equiv a^p + b^p \pmod{p}$$

Problem 12 : (8 points) Let $p \geq 5$ be a prime, and let a have order 4 modulo p. What is the least residue of $(a+1)^4 \pmod{p}$?

Since a has order 4 modulo p, $a^4 \equiv 1 \pmod{p}$.

Therefore $a^4 - 1 \equiv 0 \pmod{p}$, from which we will conclude 2 facts:

- $a^4 - 1 \equiv (a-1)(a^3+a^2+a+1) \pmod{p}$ and since $\mathbb{Z}/p\mathbb{Z}$ has no nontrivial zero divisors, it follows that either $a \equiv 1 \pmod{p}$, which is impossible since a has order 4 mod p, or $a^3+a^2+a+1 \equiv 0 \pmod{p}$.
- Also $a^4 - 1 \equiv (a^2-1)(a^2+1) \pmod{p}$. Again we may conclude that either $a^2 \equiv 1 \pmod{p}$, which is not possible since a has order 4 mod p, or $a^2 \equiv -1 \pmod{p}$

So we know both $a^3+a^2+a+1 \equiv 0 \pmod{p}$ and
$a^2 \equiv -1 \pmod{p}$

$$\begin{aligned} \text{Therefore } (a+1)^4 &\equiv a^4 + 4a^3 + 6a^2 + 4a + 1 \pmod{p} \\ &\equiv 1 + 4(a^3+a^2+a+1) + 2a^2 - 3 \pmod{p} \\ &\equiv 2(-1) - 2 \pmod{p} \\ &\equiv -4 \pmod{p} \end{aligned}$$

The least residue of $(a+1)^4$ is $p-4$. (Remember that it must be positive!)

Extra problem for graduate credit:

Problem 13 : (8 points) Throughout, let p be an odd prime, and $a \in \mathbb{Z}$ with $(a, p) = 1$. It might help to remember that in this case p has a primitive root.

a) Show that if $x^2 \equiv a \pmod{p}$ has a solution, then $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Let r be a solution, i.e. $r^2 \equiv a \pmod{p}$. Then $(r, p) = 1$ as well.

Then by Fermat's Theorem

$$1 \equiv r^{p-1} \equiv (r^2)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \pmod{p}$$

where we use that $p-1$ is even so $\frac{p-1}{2} \in \mathbb{Z}$.

b) Show that the converse is also true: If $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, then $x^2 \equiv a \pmod{p}$ has a solution.

Conversely, let g be a primitive root of p and write $a \equiv g^k \pmod{p}$ for some integer k. (This is possible since a is a unit and g is a primitive root.)

Then

$$1 \equiv a^{\frac{p-1}{2}} \equiv (g^k)^{\frac{p-1}{2}} \equiv g^{\frac{k(p-1)}{2}} \pmod{p}.$$

Since g is a primitive root, it follows that $\frac{k(p-1)}{2}$ is a multiple of $p-1$. This is only possible if $\frac{k}{2} \in \mathbb{Z}$. Then $x^2 \equiv a \pmod{p}$ has a solution, namely $x \equiv g^{k/2} \pmod{p}$.