Math 255: Spring 2017
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	4	
3	10	
4	12	
5	9	
6	6	
7	12	
8	10	
9	8	
10	10	
11	5	
12	10	
TOTAL	100	

Problem 1 : (4 points) Please compute 7^{-1} modulo 23.

$$23 = 3\cdot 7 + 2$$
$$7 = 3\cdot 2 + 1$$

$$\begin{aligned} 1 &= 7 - 3\cdot 2 \\ &= 7 - 3(23 - 3\cdot 7) \\ &= 7 - 3\cdot 23 + 9\cdot 7 \\ &= 10\cdot 7 - 3\cdot 23 \end{aligned}$$

$$7^{-1} \equiv 10 \pmod{23}$$

Problem 2 : (4 points) Prove that if a is odd, then

$$a^2 \equiv 1 \pmod 8.$$

Hint: What are the possibilities for $a \pmod 8$?

Let a be odd, so there is $n \in \mathbb{Z}$ with $a = 2n+1$

By the division algorithm, there is r with $r = 0,1,2,3$ and $n = 4q + r$. Then

$$a = 2(4q+r)+1 = 8q + 2r + 1 = \begin{cases} 8q+1 & \text{if } r=0 \\ 8q+3 & \text{if } r=1 \\ 8q+5 & \text{if } r=2 \\ 8q+7 & \text{if } r=3 \end{cases}$$

So $a \equiv 1, 3, 5$ or $7 \pmod 8$

Checking case by case, we get that $a^2 \equiv \begin{cases} 1^2 \equiv 1 \pmod 8 \\ 3^2 \equiv 1 \pmod 8 \\ 5^2 \equiv 1 \pmod 8 \\ 7^2 \equiv 1 \pmod 8 \end{cases}$

So $a^2 \equiv 1 \pmod 8$ if a is odd

Problem 3 : (10 points)

a) (4 points) If $\gcd(a, n) = 1$, please give the definition of the (multiplicative) order of a modulo n.

It is the smallest positive integer t such that

$$a^t \equiv 1 \pmod{n}$$

b) (3 points) What is the order of 3 modulo 7?

Since $\varphi(7) = 6$, the order of 3 can be 1, 2, 3 or 6

$3^1 \equiv 3 \not\equiv 1 \pmod{7}$

$3^2 \equiv 9 \equiv 2 \not\equiv 1 \pmod{7}$

$3^3 \equiv 2 \cdot 3 \equiv 6 \not\equiv \pmod{7}$

$3^6 \equiv 1 \pmod{7}$ by Fermat's Theorem, so 3 has order 6 modulo 7.

c) (3 points) What is $\log_3 6$ in $(\mathbb{Z}/7\mathbb{Z})^\times$?
Note: In the book, the author talks about the "index of 6 relative to 3 modulo 7," and uses the symbol $\text{ind}_3\, 6$. This is exactly the same thing and you can just pretend this is what it says above.

Problem 4 : (12 points) For each of the following statements, state if it is true or false. **Justify each of your answers.** There will be partial credit for this question.

a) Let φ be the Euler-φ function from class. Then $\varphi(16) = \varphi(2)\varphi(8)$.

False! $\varphi(16) = 16-8 = 8$ $\quad 8 \neq 1 \cdot 4$

$\varphi(2) = 2-1 = 1$

$\varphi(8) = 8-4 = 4$ $\quad$ (Note that $(2,8) \neq 1$)

b) The system of linear congruences

$$x \equiv 2 \pmod{12}$$
$$x \equiv 6 \pmod{15}$$

has a unique solution modulo $n = 12 \cdot 15 = 180$.

False! $(12,15)=3$ and $2 \not\equiv 6 \pmod 3$

so there is no solution.

(If there was a solution, there would be a unique solution modulo $\text{lcm}(12,15)=60$ so 3 solutions modulo 180)

c) The equation

$$2x \equiv 4 \pmod 6$$

has the unique solution $x \equiv 2 \pmod 6$.

False! Dividing through by 2 we get $x \equiv 2 \pmod 3$

so there is another solution: $x \equiv 5 \pmod 6$

d) If $x \equiv 0 \pmod 2$, then $x \equiv 2 \pmod 4$.

False! If $x \equiv 0 \pmod 2$ then this has 2 lifts:

$x \equiv 0 \pmod 4$ or $x \equiv 2 \pmod 4$

Problem 5 : (9 points)

a) (4 points) Compute gcd(36, 102). You may use any technique you like, but you must justify your answer.

$102 = 2 \cdot 36 + 30$

$36 = 30 + 6$

$30 = 5 \cdot 6$

$(36, 102) = 6$

b) (5 points) Please give all integer solutions to the linear equation

$$36x + 102y = 12.$$

$6 \mid 12$ so there are integer solutions

$6 = 36 - 30 = 36 - (102 - 2 \cdot 36) = 3 \cdot 36 - 102$

so $12 = 6 \cdot 36 - 2 \cdot 102$

and we get the particular solution $x_p = 6$, $y_p = -2$

The integer solutions are

$x = x_p + \frac{b}{(a,b)} t = 6 + 17t$

$t \in \mathbb{Z}$

$y = y_p - \frac{a}{(a,b)} t = -2 - 6t$

Problem 6 : (6 points) Consider the following system of simultaneous linear congruences:

$$x \equiv 1 \pmod 2$$
$$2x \equiv 1 \pmod 3$$
$$2x \equiv 1 \pmod 5$$

a) (1 point) There is an integer n such that there is exactly one solution to this set of congruences in $\mathbb{Z}/n\mathbb{Z}$. What is the value of n?

$n = 30$

b) (5 points) Solve this system of congruences.

First we put in "standard form":

$$x \equiv 1 \pmod 2$$
$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$

Now we apply CRT:

$M_1 = 15 \quad x_1 \equiv 15^{-1} \equiv 1^{-1} \equiv 1 \pmod 2$

$M_2 = 10 \quad x_2 \equiv 10^{-1} \equiv 1^{-1} \equiv 1 \pmod 3$

$M_3 = 6 \quad x_3 \equiv 6^{-1} \equiv 1^{-1} \equiv 1 \pmod 5$

So $x \equiv 1 \cdot 15 \cdot 1 + 2 \cdot 10 \cdot 1 + 3 \cdot 6 \cdot 1 \pmod{30}$

$\equiv 15 + 20 + 18 \pmod{30}$

$\equiv 3 + 20 \equiv 23 \pmod{30}$

Problem 8 : (10 points) Give all solutions to the following quadratic congruences.

a) $x^2 \equiv 7 \pmod{27}$ $\quad 27 = 3^3$ and 3 is odd

First we solve $x^2 \equiv 7 \equiv 1 \pmod 3$. This has solution

$x \equiv 1 \pmod 3$.

Next we solve $x^2 \equiv 7 \pmod 9$ by lifting:

$$x_1 = 1 + 3y_0 \rightsquigarrow (1+3y_0)^2 \equiv 7 \pmod 9$$

$$1 + 6y_0 + 9y_0^2 \equiv 7 \pmod 9$$

$$6y_0 \equiv 6 \pmod 9$$

$$2y_0 \equiv 2 \pmod 3$$

$$y_0 \equiv 1 \pmod 3$$

So $x_1 \equiv 1 + 3 \equiv 4 \pmod 9$

Finally we solve $x^2 \equiv 7 \pmod{27}$ by lifting:

$$x_1 = 4 + 9y_0 \rightsquigarrow (4+9y_0)^2 \equiv 7 \pmod{27}$$

$$16 + 72y_0 + 81y_0^2 \equiv 7 \pmod{27}$$

$$18y_0 \equiv -9 \pmod{27}$$

$$2y_0 \equiv -1 \equiv 2 \pmod 3$$

$$y_0 \equiv 1 \pmod 3$$

So $x_1 \equiv 4 + 9 \equiv 13 \pmod{27}$

Since 3 is odd, there are 2 solutions, $\boxed{x \equiv 13 \pmod{27} \text{ and } x \equiv -13 \equiv 14 \pmod{27}}$

8

b) $x^2 \equiv 25 \pmod{40}$ $\quad 40 = 8 \cdot 5$

So we solve

- $x^2 \equiv 25 \equiv 1 \pmod 8$. This has solutions
$$x \equiv 1, 3, 5, 7 \pmod 8$$

- $x^2 \equiv 25 \equiv 0 \pmod 5$. This has solution $x \equiv 0 \pmod 5$

Now we use CRT to get the simultaneous lifts mod 40. We have $a_1 = 1, 3, 5, 7$ and $a_2 = 0$. Since $a_2 = 0$ we don't need M_2 and x_2. We have
$$M_1 = 5 \quad x_1 \equiv 5^{-1} \equiv 5 \pmod 8$$

So the solutions are

$$x \equiv 1 \cdot 5 \cdot 5 + 0 \equiv 25 \pmod{40}$$
$$x \equiv 3 \cdot 5 \cdot 5 + 0 \equiv 75 \equiv 35 \pmod{40}$$
$$x \equiv 5 \cdot 5 \cdot 5 + 0 \equiv 125 \equiv 5 \pmod{40}$$
$$x \equiv 7 \cdot 5 \cdot 5 + 0 \equiv 175 \equiv 15 \pmod{40}$$

Problem 9 : (8 points)

a) Give all of the lifts of

$$x \equiv 2 \pmod 5$$

to values in $\mathbb{Z}/10\mathbb{Z}$. In other words, if $x \equiv 2 \pmod 5$, what can x be modulo 10?

$x \equiv 2, 7 \pmod{10}$

b) Show that any integer of the form $10k + 7$ is of the form $5j + 2$, but not conversely.

If $n = 10k+7$, $k \in \mathbb{Z}$, then

$$n = 5(2k) + 5 + 2 = 5(2k+1) + 2$$

So n is of the form $5j+2$ for $j = 2k+1$

However, $n = 12$ is of the form $5j+2$ for $j=2$

but not of the form $10k+7$ for any $k \in \mathbb{Z}$.

Problem 10 : (10 points) Let $\omega(1) = 0$ and, for $n > 1$ let $\omega(n)$ denote the number of distinct prime divisors of n. In other words, if $n = p_1^{k_1} \dots p_r^{k_r}$ is the factorization of n into distinct prime powers, $\omega(n) = r$.

a) Prove that $f(n) = 2^{\omega(n)}$ is multiplicative.

Let m,n be such that $(m,n)=1$. Then their prime-power factorizations, $m=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$ do not share

$n=q_{b_1}^{f_1}q_{b_2}^{f_2}\cdots q_{b_\ell}^{f_\ell}$

any primes $(p_i \neq q_{b_j})$. Therefore the prime-power factorization of mn is $p_1^{e_1}\cdots p_k^{e_k}q_{b_1}^{f_1}\cdots q_{b_\ell}^{f_\ell}$ and $\omega(mn)=k+\ell$. Therefore

$$f(mn)=2^{\omega(mn)}=2^{k+\ell}=2^k\cdot 2^\ell = 2^{\omega(m)}\cdot 2^{\omega(n)}$$
$$=f(m)f(n)$$

and f is multiplicative

b) Prove that $\sum_{d|n} 2^{\omega(d)}$ is multiplicative.

Problem 11 : (5 points) Prove that $\varphi(n^2) = n\varphi(n)$.

Let n have prime-power factorization

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

Then $\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$

The prime-power factorization of n^2 is

$$n = p_1^{2e_1} p_2^{2e_2} \cdots p_k^{2e_k}$$

So $\varphi(n^2) = n^2\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$

$$= n\,\varphi(n)$$

Problem 12 : (10 points)

a) State Fermat's Little Theorem (also known as Fermat's Theorem in the book).

Let p be a prime and $a \in \mathbb{Z}$ be such that $(a, p) = 1$

Then $a^{p-1} \equiv 1 \pmod{p}$

b) Let $p \equiv 3 \pmod 4$ be a prime. Let a be an integer such that $\gcd(a, p) = 1$ and assume that the equation

$$x^2 \equiv a \pmod{p}$$

has a solution. Show that

$$x \equiv a^{(p+1)/4} \pmod{p}$$

is a solution to this equation.