Math 42 – Final Exam
Friday, May 13, 2011

Name: SOLUTIONS

Upon completion of your exam, please sign below.

I have neither given nor received aid in this exam.

Signature: _____

For full credit, all work must be shown and clearly presented. No calculators.

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	

1. Does 266 have a multiplicative inverse mod 663? If the answer is yes, find the multiplicative inverse of 266 in $\mathbb{Z}_{663}$.

Decide if 266 and 663 are relatively prime:

$$663 = 2 \cdot 266 + 131$$
$$266 = 2 \cdot 131 + 4$$
$$131 = 32 \cdot 4 + 3$$
$$4 = 1 \cdot 3 + \boxed{1} \leftarrow \text{GCD}.$$
$$3 = 3 \cdot 1 + 0$$

Since $(266, 663) = 1$, 266 does have a multiplicative inverse mod 663.

	2	2	32	1	3
0 1	2	5	162	167	663
1 0	1	2	65	67	266

22 / 167 / 3 / 501 / 162

2 / 67 / 3 / 201

So $266 \cdot 167 - 663 \cdot 67 = 1$, and the inverse of 266 is $\boxed{167}$ in $\mathbb{Z}_{663}$

2. (a) Find a GCD of $4+3i$ and $5-i$ in $\mathbb{Z}[i]$.

$5-i = (4+3i)(1-i) + (-2)$

$4+3i = (-2)(-2-i) + \boxed{i}$

$-2 = i(2i) + 0$

A GCD of $4+3i$ and $5-i$ is $\boxed{i}$

$\frac{(5-i)(4-3i)}{(4+3i)(4-3i)} = \frac{17-19i}{25}$

(b) Find a solution (X, Y) with X and Y in $\mathbb{Z}[i]$ to the equation $(4+3i)X+(5-i)Y = 1$.

		$1-i$	$-2-i$	$2i$
0	1	$1-i$	$-2+i$	$-1-5i$
1	0	1	$-2-i$	$3-4i$

$(-2+i)(3-4i) - (-2-i)(-1-5i) = 1$

$(-2+i)(-i)(4+3i) + (2+i)(-i)(5-i) = 1$

So $\boxed{X = 1+2i, \quad Y = 1-2i}$ is a solution

3. Decide how many incongruent solutions there are to each of the following congruences. No partial credit will be given if no work is shown. *Note: 167 is prime.*

I $50x \equiv 17 \mod 67$

II $50x \equiv 17 \mod 166$

III $50x \equiv 16 \mod 166$

IV $x^2 \equiv 7 \mod 167$

V $x^2 \equiv 2 \mod 145$

VI $x^2 \equiv 6 \mod 145$

No solutions	II, V.
One solution	I
Two solutions	III, IV
Three solutions	
Four solutions	VI

I. $(50, 67) = 1$ and $1 \mid 17$, so there is 1 solution

II. $(50, 166) = 2$ and $2 \nmid 17$, so there are 0 solutions

III. $(50, 166) = 2$ and $2 \mid 16$, so there are 2 solutions.

IV. $\left(\frac{7}{167}\right) = -\left(\frac{167}{7}\right) = -\left(\frac{6}{7}\right) = -\left(\frac{-1}{7}\right) = -(-1) = 1$, so there are 2 solutions.

V. $145 = 5 \cdot 29$. $\left(\frac{2}{5}\right) = -1$ and $\left(\frac{2}{29}\right) = -1$, so there are no solutions.

VI. $\left(\frac{6}{5}\right) = \left(\frac{1}{5}\right) = 1$ and $\left(\frac{6}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{3}{29}\right) = -\left(\frac{3}{29}\right) = -\left(\frac{29}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1$,
so there are 4 solutions.

4. Find all incongruent solutions to the equation

$$x^2 \equiv 11 \mod 95.$$

$95 = 5 \cdot 19$, so solve mod 5 and mod 19 first

$x^2 \equiv 11 \mod 5 \longrightarrow x^2 \equiv 1 \mod 5$

So $x \equiv \pm 1 \mod 5$

$x^2 \equiv 11 \mod 19 \longrightarrow x^2 = 11, 30, 49, \ldots$

So $x \equiv \pm 7 \mod 19$.

Use Chinese remainder theorem to get solutions mod 95.

Find $a \equiv 1 \mod 5$, $0 \mod 19$: $a = -19$

Find $b \equiv 0 \mod 5$, $1 \mod 19$: $b = 20$.

So $x \equiv -19 + 7(20) = 121 \mod 95$

or $x \equiv -19 - 7(20) = -159 \mod 95$

or $x \equiv 19 + 7(20) = 159 \mod 95$

or $x \equiv 19 - 7(20) \equiv -121 \mod 95$

That is, $\boxed{x \equiv 26, 64, 31, 69 \mod 95}$

Here is a table of powers of 3 mod 31. Use it to solve the next two questions.

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3^a	3	9	27	19	26	16	17	20	29	25	13	8	24	10	30

a	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
3^a	28	22	4	12	5	15	14	11	2	6	18	23	7	21	1

5. Use logarithms to find all incongruent solutions to the congruence

$$5x^6 \equiv 10 \mod 31.$$

$\log_3(5x^6) \equiv \log_3 10 \mod 30$

$\log_3 5 + 6\log_3 x \equiv 14 \mod 30$

$20 + 6\log_3 x = 14 + 30k, \quad k \in \mathbb{Z}$

$6\log_3 x = -6 + 30k$

$\log_3 x = -1 + 5k = 4, 9, 14, 19, 24, 29, \ldots$

So $\boxed{x \equiv 19, 29, 10, 12, 2, 21 \mod 31}$

6. What is the order of 25^{26} in U_{31}? What is the order of 26^{25} in U_{31}?

$25 \equiv 3^{10} \mod 31$, so $25^{26} \equiv 3^{260} \equiv 3^{20} \mod 31$

Order of $3^{20} = \frac{30}{(30,20)} = \frac{30}{10} = \boxed{3}$

$26^{25} \equiv (3^5)^{25} \mod 31$, so $26^{25} \equiv 3^{125} \equiv 3^5 \mod 31$.

Order of $3^5 = \frac{30}{(30,5)} = \frac{30}{5} = \boxed{6}$.

7. Express $\sqrt{15}$ as a simple continued fraction.

$$\sqrt{15} = 3 + (\sqrt{15} - 3) = 3 + \cfrac{1}{\cfrac{1}{\sqrt{15}-3}} = 3 + \cfrac{1}{\cfrac{\sqrt{15}+3}{6}}$$

$$= 3 + \cfrac{1}{1 + \cfrac{\sqrt{15}-3}{6}} = 3 + \cfrac{1}{1 + \cfrac{1}{\cfrac{6}{\sqrt{15}-3}}} = 3 + \cfrac{1}{1 + \cfrac{1}{\cfrac{6(\sqrt{15}+3)}{6}}}$$

$$= 3 + \cfrac{1}{1 + \cfrac{1}{\sqrt{15}+3}} = 3 + \cfrac{1}{1 + \cfrac{1}{6 + \cfrac{1}{1 + \cfrac{1}{6 + \ddots}}}}$$

So $\boxed{\sqrt{15} = [3, \overline{1, 6}]}$.

8. Find two units in $\mathbb{Z}[\sqrt{15}]$, neither of which is ± 1. Your two units may not be conjugates or additive inverses (that is, if one of your units is $x + y\sqrt{15}$, your other unit may not be $x - y\sqrt{15}$, $-x - y\sqrt{15}$, or $-x + y\sqrt{15}$.)

We need to solve $x^2 - 15y^2 = \pm 1$

	3	1	6	...
0 1	3	4	27	...
1 0	1	1	7	

$4^2 - 15 \cdot 1^2 = 1$, so $4 + \sqrt{15}$ is a unit in $\mathbb{Z}[\sqrt{15}]$.

$(4+\sqrt{15})^k$ is a unit for any $k \in \mathbb{Z}$, so to find a second unit, take $k = 2$.

$$(4+\sqrt{15})^2 = 16 + 15 + 8\sqrt{15} = 31 + 8\sqrt{15}.$$

$\boxed{4 + \sqrt{15} \text{ and } 31 + 8\sqrt{15}}$ are two units in $\mathbb{Z}[\sqrt{15}]$.

9. Given $u \in U_p$ with order d, prove that if $u^n \equiv 1 \mod p$, then d divides n.

Use division with remainder: $n = dq + r$ for some q, r in $\mathbb{Z}$ s.t. $0 \leq r < d$.

Then $u^n \equiv 1 \mod p \Rightarrow u^{dq+r} = u^{dq} u^r \equiv 1 \mod p$.

But if u has order d, $u^{dq} = (u^d)^q \equiv 1^q \equiv 1 \mod p$.

So $u^r \equiv 1 \mod p$.

If $r \in \mathbb{N}$, then r would be a natural number smaller than the order of u with $u^r \equiv 1 \mod p$, which would contradict the definition of order.

Thus, $r \notin \mathbb{N}$ and since $0 \leq r < d$, r must be 0.

So $n = dq + 0$, i.e. $n = dq$ and $d \mid n$ by the definition of divides.

10. Prove that there are infinitely many primes of the form $6k + 5$.

Suppose there are finitely many such primes, $p_1, p_2, \cdots, p_k$.

Consider $n = 6p_1p_2 \cdots p_k - 1$. Clearly, $n \equiv 5 \bmod 6$ and $p_i \nmid n$ for $i = 1, 2, \ldots, k$.

If n is prime, we've produced a new prime of the form $6k+5$, and we're done.

If n is not prime, factor it. Since $n = 6k+5$ for some $k \in \mathbb{Z}$, n is odd and has prime factors which must be of the form $6k+1$, $6k+3$ or $6k+5$. Since the only way to get something $5 \bmod 6$ as a product of factors congruent to 1, 3 or 5 mod 6 is to have at least one factor congruent to 5 mod 6, we see that there is some prime p s.t. $p \mid n$ and $p \equiv 5 \bmod 6$. Again, we've produced a new prime of the form $6k+5$, and we're done.

In summary, there cannot be finitely many primes of the form $6k+5$, as desired.

11. Prove that for an odd prime p, if $p \equiv 1 \mod 4$, then

$$\sum_{r=1}^{p-1} r\left(\frac{r}{p}\right) = 0.$$

Notice that if $p \equiv 1 \bmod 4$, then $\left(\frac{-1}{p}\right) = 1$.

This implies that $\left(\frac{r}{p}\right) = \left(\frac{-r}{p}\right) = \left(\frac{p-r}{p}\right)$.

So our sum can be rewritten:

$$\sum_{r=1}^{p-1} r\left(\frac{r}{p}\right) = \sum_{r=1}^{\frac{p-1}{2}} \left[r\left(\frac{r}{p}\right) + (p-r)\left(\frac{p-r}{p}\right) \right]$$

$$= \sum_{r=1}^{\frac{p-1}{2}} \left[(r + (p-r))\left(\frac{r}{p}\right) \right]$$

$$= \sum_{r=1}^{\frac{p-1}{2}} p \cdot \left(\frac{r}{p}\right)$$

Now we know that mod p there are $\frac{p-1}{2}$ squares, and since $p \equiv 1 \bmod 4$, $\left(\frac{r}{p}\right) = \left(\frac{-r}{p}\right) \Rightarrow$ there are $\frac{p-1}{4}$ squares in the "first half," i.e. among $1, 2, 3, \ldots, \frac{p-1}{2}$, there are $\frac{p-1}{4}$ quadratic residues and $\frac{p-1}{4}$ quadratic non-residues.

Thus $\sum_{r=1}^{\frac{p-1}{2}} p\left(\frac{r}{p}\right) = p \cdot \left(\frac{p-1}{4}\right) - p\left(\frac{p-1}{4}\right) = 0.$

So $\sum_{r=1}^{p-1} r\left(\frac{r}{p}\right) = 0$, as desired.