A 55 - 60

A- 49 - 54

B starts at 30

C starts at 20

Pries: 405 Number Theory

Midterm: Spring 2012

This midterm has 7 short problems (each worth 5 points) and 3 long problems (each worth 15 points). You can skip 1 short and 1 long problem, so a perfect score is 60 points. Give one sentence explanation for the short problems and a complete explanation for the long problems. Read the exam carefully before you begin.

Short problems:

1. Is 42 a unit modulo 99?

No $\gcd(42, 99) = 3$

$\nexists$ solution to $42x + 99y = 1$ w/ $x, y \in \mathbb{Z}$

$\nexists$ solution to $42x \equiv 1 \mod 99$

2. Find $\phi(180)$.

$180 = 18 \cdot 10 = 9 \cdot 4 \cdot 5$

$\phi(180) = \phi(9)\phi(4)\phi(5) = 6 \cdot 2 \cdot 4 = 48$

3. Find a number x between 0 and 179 so that $x \equiv 3^{100} \mod 180$.

$3^{100} = 3^{98} \cdot 3^{98} \cdot 3^{4} \equiv 1 \cdot 1 \cdot 81$

$81 \mod 180$

1. Are there infinitely many primes congruent to 1 modulo 4?

Yes - If not, let $p_1 \cdots p_n$ be the list

$N = (2p_1 \cdots p_n)^2 + 1$

Let $q \mid N$ q prime then q odd & $q \nmid 2p_1 \cdots p_n$

$-1 \equiv 1 \pmod{q}$

so $q \equiv 1 \pmod 4$ new prime

5. Does $x^2 \equiv 15 \bmod 103$ have a solution?

$$\left(\frac{15}{103}\right) = \left(\frac{5}{103}\right)\left(\frac{3}{103}\right) = \left(\frac{103}{5}\right)\left(\frac{103}{3}\right)(-1) = \left(\frac{3}{5}\right)\left(\frac{1}{3}\right)(-1)$$

$$= -1 \cdot 1(-1) = 1$$

yes

6. Factor 7 in $\mathbb{Z}[\sqrt{2}]$. $= \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$

$7 = (3 - \sqrt{2})(3 + \sqrt{2})$

7. Does $x^2 - 2y^2 \equiv 13$ have a solution with $x, y \in \mathbb{Z}$?

No $x^2 \equiv 2y^2 \pmod{13}$

$2 - \frac{x^2}{y^2} \equiv 2$

but $13 \equiv 5 \pmod 8$ & $2 \neq 5 \pmod{13}$

Long problems:

Pooh was saying to himself, "If only I could think of something!" For he felt sure that a Very Clever Brain could catch a Heffalump if only he knew the right way to go about it.
– A.A. Milne.

1. Here is a table of the powers of 2 modulo 11. Notice that $2^6 = 9 \bmod 11$.

i	1	2	3	4	5	6	7	8	9	10
2^i	2	4	8	5	10	9	7	3	6	1

(a) Solve $x^3 \equiv 9 \bmod 11$.

$x^3 \equiv 2^6 \bmod 11$

$x \equiv 2^2 = 4 \bmod 11$

4

(b) What is the order of 9 mod 11?

$9^1 = 2^6$

$9^2 = 2^{12} = 2^2$

$9^3 = 2^8$

$9^4 = 2^{14} = 2^4$

$9^5 = 2^{10} = 1$

5

(c) What is the multiplicative inverse of 9 modulo 11?

$2^6 \cdot 2^4 = 2^{10} \equiv 1 \bmod 11$

$9 \cdot 5 \equiv 1 \bmod 11$

5

II. Prove Euler's criterion, $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$, using these steps:

(a) If p is a prime and $x^2 \equiv 1 \bmod p$, prove that $x \equiv \pm 1 \bmod p$.

$p \mid (x^2-1)$ so $p \mid (x-1)(x+1)$

By prime claim, $p \mid (x-1)$ or $p \mid (x+1)$

So $x \equiv 1 \bmod p$ or $x \equiv -1 \bmod p$

(b) If g is a primitive root modulo p, prove that $g^{(p-1)/2} \equiv -1 \bmod p$.

$g^{p-1} \equiv 1 \bmod p$ by Fermat's Little Thm.

So if $x = g^{\frac{p-1}{2}}$ then $x^2 \equiv 1 \bmod p$

By part (a), $x \equiv 1 \bmod p$ or $x \equiv -1 \bmod p$

$g^{\frac{p-1}{2}} = x \equiv 1 \bmod p$ impossible since g primitive root.

So $g^{\frac{p-1}{2}} \equiv -1 \bmod p$.

(c) Prove that a is a square modulo p if and only if $a^{(p-1)/2} \equiv 1 \bmod p$.

If $a = y^2$ is a square, then $a^{\frac{p-1}{2}} = y^{p-1} \equiv 1 \bmod p$

If $a \neq 0$, then $a = g^c$ where c odd

write $c = 2k+1$

so $a^{\frac{p-1}{2}} = g^{2k\left(\frac{p-1}{2}\right)} \cdot g^{\frac{p-1}{2}}$

$a^{\frac{p-1}{2}} = 1 \cdot (-1)$ by part b

So $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$.

III. Let $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. You can assume that $\mathbb{Z}[i]$ has a Euclidean algorithm, so that greatest common divisors exist. This means that Bezout's lemma is true in $\mathbb{Z}[i]$ which says that $\gcd(\alpha, \beta) = 1$ if and only if there is a solution $\alpha x + \beta y = 1$ with $x, y \in \mathbb{Z}[i]$.

(a) Suppose p is a prime of $\mathbb{Z}[i]$ and $\alpha, \beta \in \mathbb{Z}[i]$. If $p \mid \alpha\beta$, prove that $p \mid \alpha$ or $p \mid \beta$ (Prime claim).

If $p \mid \alpha$ done.
If not, $\gcd(p, \alpha) = 1$ so $\exists$ solution $\alpha x + py = 1$

so $\alpha\beta x + p\beta y = \beta$
so $pkx + p\beta y = \beta$
so $p(kx + \beta y) = \beta$ so $p \mid \beta$

(b) If $p \equiv 1 \bmod 4$, prove that there is an integer x such that $x^2 + 1$ is a multiple of p.

If $p \equiv 1 \bmod 4$ Hint: use $-1 \neq 0$ mod p
then $-1 \equiv x^2 \bmod p$ has a solution.
then $p \mid (x^2 + 1)$ so $p \mid (x+i)(x-i)$
By part (a) So $x^2 + 1$ is a multiple of p.

(c) Use parts (a) and (b) to prove that if $p \equiv 1 \bmod 4$, then p is not prime in $\mathbb{Z}[i]$.

So $p \mid (x+i)(x-i)$ by part b

If p prime in $\mathbb{Z}$, by part a, $p \mid (x+i)$ or $p \mid (x-i)$.

But $x+i$ not a multiple of p in $\mathbb{Z}[i]$
$x-i$ " " " " " " in $\mathbb{Z}[i]$

Contradiction, so p not prime.