SECOND MIDTERM
MATH 104C, UCSD, SPRING 18

You have 80 minutes.

There are 6 problems, and the total number of points is 70. Show all your work. *Please make your work as clear and easy to follow as possible.*

Name:______________________________

Signature:______________________________

Student ID #:______________________________

Problem	Points	Score
1	15	
2	10	
3	15	
4	10	
5	10	
6	10	
7	10	
8	10	
Total	70	

1. (15pts) (i) *Give the definition of the p-adic valuation of an integer.*

If n is an integer and we write $n = p^e m$ where $(m, p) = 1$ then e is the p-adic valuation of n.

(ii) *Give the definition of the norm of an element of* $\mathbb{Z}[\sqrt{d}]$.

If $\alpha = x + y\sqrt{d}$ then $\bar{\alpha} = x - y\sqrt{d}$ and

$$\begin{aligned} N(\alpha) &= \alpha\bar{\alpha} \\ &= x^2 - y^2 d. \end{aligned}$$

(iii) *Give the definition of the fundamental solution of Pell's equation* $x^2 - dy^2 = 1$.

The fundamental solution $\delta = x + y\sqrt{d}$ of Pell's equation has the property that $x > 0$ and $y > 0$ and δ is minimal subject to these conditions.

2. (10pts) *If α is a 5-adic integer such that*

$$\alpha^2 \in -1 \qquad \text{and} \qquad \alpha = 3 + a_1 \cdot 5 + a_2 \cdot 5^2 + a_3 \cdot 5^3 + \dots$$

then determine a_1, a_2 and a_3.

Note that $3^2 = 9 \equiv 4 \mod 5$, so the first coefficient is indeed correct. Let $f(x) = x^2 + 1$. Then $f'(x_0) = 2x_0$. We want to choose t so that $3 + 5t$ satisfies the equation

$$(3^2 + 1) + (2 \cdot 3) \cdot 5 \cdot t \equiv 0 \mod 5^2.$$

This reduces to

$$6t \equiv -2 \mod 5,$$

so that $t = 3$. Next we want to choose t so that $3 + 3 \cdot 5 + t \cdot 5^2$ satisfies

$$(3 + 3 \cdot 5)^2 + 1 + 2 \cdot (3 + 3 \cdot 5)t \cdot 5^2 \equiv 0 \mod 5^3.$$

This reduces to

$$13 + 6t \equiv 0 \mod 5,$$

so that $t = 2$.
Finally we want to choose t so that $3 + 3 \cdot 5 + 2 \cdot 5^2 + t \cdot 5^3$ satisfies

$$(3 + 3 \cdot 5 + 2 \cdot 5^2)^2 + 1 + 2 \cdot 3(3 + 3 \cdot 5 + 2 \cdot 5^2)t \equiv 0 \mod 5.$$

This reduces to

$$37 + 6t \equiv 0 \mod 5,$$

so that $t = 3$.
Thus

$$a_1 = 3 \qquad a_2 = 2 \qquad \text{and} \qquad a_3 = 3.$$

3. (15pts) (i) *State Legendre's theorem.*

If a, b and c are square-free, relatively coprime integers then the equation

$$ax^2 + by^2 + cz^2 = 0$$

has a solution if and only if a, b and c don't all have the same sign and $-bc$, $-ca$, $-ab$ are quadratic residues of $|a|$, $|b|$ and $|c|$.

Decide whether the equations have non-trivial integer solutions:
(ii)

$$5x^2 - 3y^2 + 2z^2 = 0.$$

$a = 5$, $b = -3$ and $c = 2$ certainly don't all have the same sign; $6 \equiv 1 = 1^2$ is a quadratic residue of 5, but $-10 \equiv 2$ is not a quadratic residue of 3. Thus this equation does not have any integer solutions.

(iii)

$$7x^2 - y^2 + 2z^2 = 0.$$

$a = 7$, $b = -1$ and $c = 2$ certainly don't all have the same sign; $2 \equiv 9 = 3^2$ is a quadratic residue of 7; $|b| = 1$ and so there is nothing to check for -14; $7 \equiv 1 \mod 2$ is a quadratic residue. Thus this equation does have integer solutions.
In fact $x = z = 1$ and $y = 3$ is one solution.

4. (10pts) *Show that if* $\xi \in \mathbb{R}$ *and* $t \in \mathbb{N}$ *then we may find integers* x *and* $0 < y \leq t$ *such that*

$$|y\xi - x| < \frac{1}{t}.$$

Consider the fractional parts $\{\, i \cdot \xi \,\}$, for $0 \leq i \leq t$. These belong to the interval $[0, 1)$. As there $t + 1$ choices for i and the union of the t intervals $[(l-1)/t, l/t)$ is $[0, 1)$, it follows that two fractional parts must lie in the same interval, so that

$$|\{\, j \cdot \xi \,\} - \{\, i \cdot \xi \,\}| < \frac{1}{t},$$

where $0 \leq i < j \leq t$. Let

$$y = j - i \in \mathbb{N} \qquad \text{and} \qquad x = \llcorner j \cdot \xi \lrcorner - \llcorner i \cdot \xi \lrcorner \in \mathbb{Z}.$$

Then $y \leq t$ and

$$\begin{aligned} y\xi - x &= j \cdot \xi - i \cdot \xi - x \\ &= j(\llcorner \xi \lrcorner + \{\, \xi \,\}) - i(\llcorner \xi \lrcorner + \{\, \xi \,\}) - x \\ &= (j \cdot \llcorner \xi \lrcorner - i \cdot \llcorner \xi \lrcorner) - x + j \cdot \{\, \xi \,\} - i \cdot \{\, \xi \,\} \\ &= j \cdot \{\, \xi \,\} - i \cdot \{\, \xi \,\}. \end{aligned}$$

5. (10pts) *Prove that the circle* $x^2 + y^2 = r$ $(r > 0)$ *is a curve of genus zero but that if* $r = 3$ *then there is no parametrisation* $x = \phi(t)$ *and* $y = \psi(t)$ *by rational functions with rational coefficients.*

Look at lines through the point $(-\sqrt{r}, 0)$,

$$y = m(x + \sqrt{r}).$$

These intersect the circle at one further point. We get

$$x^2 + m^2(x + \sqrt{r})^2 = r,$$

so that

$$(1 + m^2)x^2 + 2m^2\sqrt{r}x + m^2 r = r.$$

Thus

$$x^2 + \frac{2m^2\sqrt{r}}{1 + m^2}x + \frac{m^2 - 1}{m^2 + 1}r = 0.$$

As one of the roots is $-\sqrt{r}$ and the product of the roots is

$$\frac{m^2 - 1}{m^2 + 1}r$$

we see that x is a rational function of m. It follows that y is also a rational function of m. Thus we have a curve of genus zero.

Suppose $(x = \phi(t), y = \psi(t))$ are rational functions with rational coefficients. The denominators of $\phi(t)$ and $\psi(t)$ are polynomials in t. Therefore there are only finitely many values of t such that $\phi(t)$ and $\psi(t)$ are not defined.

Pick a rational number $t = q$ not equal to one of these values. The corresponding point (x, y) is a rational point. Clearing denominators in the usual way, we would get an integer solution of the equation

$$x^2 - 3y^2 + z^2 = 0.$$

As -1 is not a quadratic residue of 3 this contradicts Legendre's theorem.

6. (10pts) *Show that a p-adic number*

$$\alpha = p^n(a_0 + a_1 \cdot p + a_2 \cdot p^2 + a_3 \cdot p^3 + \dots)$$

represents a rational if and only if $a_1, a_2, \dots$ is eventually periodic.

There is no harm in assuming that $n = 0$ so that α is a p-adic integer. If $a_0, a_1, a_2, \dots$ is eventually periodic then α is a sum of an integer (which is the same as p-adic integer with only finitely many non-zero terms) plus finitely many p-adic integers of the form

$$\beta = 1 + p^k + p^{2k} + p^{3k} + \dots.$$

Note that

$$\beta - 1 = p^k \beta.$$

Thus

$$\beta = \frac{-1}{p^k - 1}$$

is a rational number. As a sum of rational numbers is rational, it follows that α is a rational number.
Conversely, suppose that a/b is rational number. As the sum of periodic number is periodic, we may assume that $a = 1$. Note that multiplying by -1 does not change whether or not $a_0, a_1, a_2, \dots$ is eventually periodic. So we may assume that $a = -1$. We may also assume that b is coprime to p. Note that

$$p^{\varphi(b)} \equiv 1 \mod b,$$

by Euler's theorem, so that b divides $p^k - 1$, where $k = \varphi(b)$. But then

$$\frac{1}{b} = \frac{c}{p^k - 1},$$

where $c > 0$ is an integer, and we are done by what we already proved.

Bonus Challenge Problems

7. (10pts) *If d is square-free then show that the solutions of*

$$x^2 - dy^2 = 1$$

is naturally a group isomorphic to $\mathbb{Z} \times \mathbb{Z}_2$. You may assume that there is a non-trivial solution.

See lecture 12.

8. (10pts) *Prove Legendre's theorem.*

See lecture 7.