Math 40520 Theory of Number
Homework 1

Due Wednesday, 2015-09-09, in class

Do 5 of the following 7 problems. Please only attempt 5 because I will only grade 5.

1. Find all rational numbers x and y satisfying the equation $x^2 + y^2 = 5$. [Hint: Use the change of variables $u = x - 2y$ and $v = 2x + y$ and find an equation relating u and v.]

   Proof. Via the change of variables we get $u^2 + v^2 = 5x^2 + 5y^2 = 25$ so $(u/5)^2 + (v/5)^2 = 1$. We already know that the rational solutions to this equation are of the form $u/5 = 2t/(t^2 + 1)$ and $v/5 = (t^2 - 1)/(t^2 + 1)$ where $t \in \mathbb{Q}$ or $t = \infty$. Thus

   $$x - 2y = u = \frac{10t}{t^2 + 1}$$
   $$2x + y = v = \frac{5(t^2 - 1)}{t^2 + 1}$$

   Solving the system of equations we get

   $$x = \frac{2(t^2 + t - 1)}{t^2 + 1}$$
   $$y = \frac{t^2 - 4t - 1}{t^2 + 1}$$

   $\square$

2. Find all rational numbers x and y satisfying the equation $x^2 + 2xy + 3y^2 = 2$. [Hint: Use the change of variables $u = x + y$ and $v = y$ and find an equation relating u and v. Then mimick how we found all Pythagorean triples.]

   Proof. Via the change of variables we get $u^2 + 2v^2 = x^2 + 2xy + 3y^2 = 2$ which has $(0, 1)$ as a solution. If $(u, v) \neq (0, 1)$ is another solution let t be the x-coordinate of the intersection between the x-axis and the line through the pole $(0, 1)$ and the point (u, v). Exactly as in the case of Pythagorean triples (the equation $x^2 + y^2 = 1$) we get, using similar triangles, that

   $$v = 1 - \frac{u}{t}$$

   Substituting we get

   $$2 = u^2 + 2v^2 = u^2 + 2(1 - \frac{u}{t})^2 = u^2(1 + 2/t^2) - 4u/t + 2$$

   and so

   $$u^2(1 + 2/t^2) = 4u/t$$

Either $u = 0$ or we can divide by u to get

$$u = \frac{4t}{t^2 + 2}$$

The case $u = 0$ is obtained by $t = 0$ or $t = \infty$ and so it's incorporated in the above formula anyway. Then we get

$$v = 1 - u/t = \frac{t^2 - 2}{t^2 + 2}$$

and these are all the rational solutions.

Now we solve

$$\begin{aligned} x + y &= \frac{4t}{t^2 + 2} \\ y &= \frac{t^2 - 2}{t^2 + 2} \end{aligned}$$

to get

$$\begin{aligned} x &= \frac{-t^2 + 4t + 2}{t^2 + 2} \\ y &= \frac{t^2 - 2}{t^2 + 2} \end{aligned}$$

which yield all rational solutions as $t \in \mathbb{Q} \cup \{\infty\}$. $\square$

3. Consider the diophantine equation

$$3x + 5y + 7z = 2$$

(a) Find a solution with $x, y, z \in \mathbb{Z}$. [Hint: Use the Euclidean algorithm from class.]

(b) Show that if $3X + 5Y + 7Z = 0$ for some integers X, Y, Z then 3 must divide $Z - Y$.

(c) Find all integral solutions to the equation.

Proof. (a) From class we know that $3 \cdot 2 + 5 \cdot (-1) = 1$ and so $(2, -1, 0)$ is a solution. Or you could have used the Euclidean algorithm from the version of Bezout's formula for 3 integers.

(b) Working modulo 3 we have

$$3x + 5y + 7z \equiv 0 \cdot x + 1 \cdot y + (-1) \cdot z \equiv y - z \pmod 3$$

so any integral solution to $3x + 5y + 7z = 0$ would have $3 \mid y - z$.

(c) We want to parametrize integral solutions (x, y, z) to $3x + 5y + 7z = 2$. As in class (where we did $3x + 5y = 1$) we subtract from this the guessed solution to obtain the equation

$$3(x - 2) + 5(y + 1) + 7z = 0$$

and from part (b) we know that $y + 1 \equiv z \pmod 3$. This implies that there must exist an integer k such that $y + 1 = z + 3k$. Plugging back into the equation we get

$$0 = 3(x - 2) + 5(y + 1) + 7z = 3(x - 2) + 5(z + 3k) + 7z = 3(x - 2) + 12z + 15k$$

and dividing by 3 we get

$$x - 2 + 4z + 5k = 0$$

so $x = 2 - 4z - 5k$. Thus all integral solutions are of the form

$$(x, y, z) = (2 - 4z - 5k, z + 3k - 1, z)$$

as $k, z \in \mathbb{Z}$.

$\square$

4. Consider the diophantine equation
$$xy = zt$$
with $x, y, z, t \in \mathbb{Z}$. Show that there exist integers a, b, c, d such that $x = ab$, $y = cd$, $z = ac$, $t = bd$. [Hint: Factor x, y, z, t into primes.]

Proof. **First solution:** If $z = 0$ then $x = 0$ or $y = 0$. Reordering we may assume that $x = 0$. Then take $a = 0$, $c = y$, $b = t$ and $d = 1$. Similarly if $y = 0$ we get the desired expression.

If $y, z \neq 0$ then we may divide to get
$$\frac{x}{z} = \frac{t}{y} = q$$
with rational q. Writing $q = b/c$ in lowest terms (with b and c coprime) we know that
$$\frac{x}{z} = \frac{b}{c} \qquad \frac{t}{y} = \frac{b}{c}$$
and there must exist integers a and d such that $x = ab$, $z = ac$, $t = db$, $y = dc$ as the numerator and denominator of a fraction are the same multiple of the numerator and denominator written in lowest terms.

Second solution: First, let's assume that x, y, z, t are all powers of a fixed prime p. So $x = p^X$, $y = p^Y$, $z = p^Z$ and $t = p^T$. The equation is then $p^{X+Y} = p^{Z+T}$, i.e., $X + Y = Z + T$. We seek to write
$$\begin{aligned} x = p^X &= ab = p^{A+B} \\ y = p^Y &= cd = p^{C+D} \\ z = p^Z &= ac = p^{A+C} \\ t = p^T &= bd = p^{B+D} \end{aligned}$$
in other words we seek to solve
$$\begin{aligned} A + B &= X \\ C + D &= Y \\ A + C &= Z \\ B + D &= T \end{aligned}$$
in the nonnegative integers. Reordering we may assume that $X \leq Z$ in which case the equation $X + Y = Z + T$ implies YT. Take $B = 0$. Then immediately $A = X$ and $D = T$ and so $C = Y - T$. All of these are nonnegative solutions as desired.

Now for the general case. For an integer n and a prime p write n_p for the power of p that shows up in the factorization of n into primes. As prime factorization is unique if $xy = zt$ we deduce that $x_p y_p = z_p t_p$ and so the first case above implies that $x_p = a_p b_p$, $y_p = c_p d_p$, $z = a_p c_p$ and $t = b_p d_p$. Then take $a = \prod a_p$, $b = \prod b_p$, $c = \prod c_p$, and $d = \prod d_p$ to get the desired expression.

Third solution: Take $a = (x, z)$ and $d = (y, t)$. Then $x = ab$ and $z = ac$ for coprime integers b and c. We get $xy = aby = zt = act$ so $by = ct$. As b and c are coprime we deduce that $b \mid t$ and $c \mid y$. Writing $y = cd$ for an integer d we immediately get $t = bd$. $\square$

5. Show that all the solutions to the diophantine equation
$$x^2 + y^2 = z^2 + t^2$$

are of the form

$$x = \frac{mn+pq}{2} \qquad y = \frac{mp-nq}{2}$$
$$z = \frac{mp+nq}{2} \qquad t = \frac{mn-pq}{2}$$

for integers m, n, p, q such that the above formulae yield integers. [Hint: Use the previous exercise.]

Proof. Rewrite the equation as $x^2 - t^2 = z^2 - y^2$ which is equivalent to

$$(x+t)(x-t) = (y+z)(z-y)$$

From the previous exercise there exist integers m, n, p, q such that

$$x + t = mn$$
$$x - t = pq$$
$$y + z = mp$$
$$z - y = nq$$

Solving the system yields the desired expressions. □

6. In this exercise you will solve the equation

$$x^2 + y^2 + z^2 = 1$$

with $x, y, z \in \mathbb{Q}$.

(a) Suppose $(x, y, z) \neq (0, 0, 1)$ is a solution. Let (a, b) be the point of intersection of the (xy)-plane with the line through (x, y, z) and $(0, 0, 1)$. Show that

$$\frac{x}{a} = \frac{y}{b} = 1 - z$$

(b) Show, mimicking the procedure from the Pythagorean triples case, that every rational solution of the diophantine equation (other than $(0, 0, 1)$) is of the form

$$x = \frac{2a}{1+a^2+b^2} \qquad y = \frac{2b}{1+a^2+b^2} \qquad z = \frac{a^2+b^2-1}{1+a^2+b^2}$$

for rationals a, b.

Proof. (a) Projecting to the (xz)-plane, i.e., with $y = 0$, we get similar right triangle with legs $1 - z$, x and 1, a. Thus $1 - z = x/a$. Similarly we get the other equation.

(b) Note that $x/a = y/b$ and so $y = bx/a$. We have

$$1 = x^2 + y^2 + z^2 = x^2 + b^2x^2/a^2 + (1 - x/a)^2$$

and so

$$x^2(1 + b^2/a^2 + 1/a^2) = 2x/a$$

Either $x = 0$ or $x = \frac{2a}{a^2+b^2+1}$ and the former case is a special example of the latter. Now compute

$$y = bx/a = \frac{2b}{a^2+b^2+1}$$

and

$$z = 1 - x/a = \frac{a^2+b^2-1}{a^2+b^2+1}$$

□

7. Suppose two of the integers $a_1, a_2, \ldots, a_n$ are coprime. Suppose $x_1 = u_1, \ldots, x_n = u_n$ is an integral solution to the diophantine equation

$$a_1x_1 + \cdots + a_nx_n = b$$

Find all the other solutions. [Hint: Cf. exercise 3.]

Proof. As in Exercise 3 we can rewrite the equation as

$$\sum a_ix_i = d = \sum a_iu_i$$

or equivalently

$$\sum a_i(x_i - u_i) = 0$$

Suppose for simplicity that a_1 and a_2 are coprime (otherwise simply reorder the indices). Then a_2 is invertible modulo a_1 and there exists $b \in \mathbb{Z}$ such that $a_2b \equiv 1 \pmod{a_1}$. If $x_1, \ldots, x_n$ is a solution then reducing modulo a_1 we get

$$\sum_{i=2}^{n} a_i(x_i - u_i) \equiv 0 \pmod{a_1}$$

and multiplying with b we get

$$x_2 - u_2 = \equiv -\sum_{i=3}^{n} ba_i(x_i - u_i) \pmod{a_1}$$

Thus we may write

$$x_2 - u_2 = a_1k - \sum_{i=3}^{n} ba_i(x_i - u_i)$$

for some integer k. Plugging it back into the equation we get

$$a_1(x_1 - u_1) + a_2(a_1k - \sum_{i=3}^{n} ba_i(x_i - u_i)) + \sum_{i=3}^{n} a_i(x_i - u_i) = 0$$

and so

$$x_1 - u_1 = -a_2k + \sum_{i=3}^{n} \frac{ba_2 - 1}{a_1} a_i(x_i - u_i)$$

where all coefficients are now integers as $ba_2 \equiv 1 \pmod{a_1}$. Thus every solution is of the form $(x_1, \ldots, x_n)$ where

$$x_1 = u_1 - a_2k + \sum_{i=3}^{n} \frac{ba_2 - 1}{a_1} a_i(x_i - u_i)$$

$$x_2 = u_2 + a_1k - \sum_{i=3}^{n} ba_i(x_i - u_i)$$

for $k, x_3, \ldots, x_n \in \mathbb{Z}$. $\square$