Math 40520 Theory of Number
Homework 2

Due Wednesday, 2015-09-16, in class

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

1. Consider the polynomials $P(X) = X^7 + 6X^6 + 3X^5 + X^4 + 5X^3 + 3X^2 + 5X + 4$ and $Q(X) = X^5 + 4X^4 + 4X^2 + X + 1$ with coefficients in $\mathbb{Z}_7$ (modulo 7). Use the Euclidean algorithm to:

   (a) Determine (P, Q). (Recall our convention that the gcd of two polynomials is the monic polynomial of highest degree dividing both of them.)

   (b) Find two polynomials $U(X)$ and $V(X)$ with coefficients in $\mathbb{Z}_7$ such that $PU + QV = (P, Q)$.

2. Show that the equation
$$x^2 + y^2 + z^2 = 20152015$$
has no integral solutions. [Hint: Try congruences modulo powers of 2.]

3. Show that the equation
$$x^{216} - y^{216} + z^{216} - t^{216} = 5$$
has no integral solutions. [Hint: Use the Euler theorem modulo 9.]

4. Consider the diophantine equation
$$2x^2 + 7y^2 = 1$$

   (a) Show that it has no integral solutions but that it has $(1/3, 1/3)$ as a rational solution.

   (b) Suppose $n \geq 2$ is an integer not divisible by 3. Show that there exist integers x, y such that
$$2x^2 + 7y^2 \equiv 1 \pmod{n}$$
   [Hint: Use the rational solution from above.]

5. This is Exercise 4.3 on page 71. Let p be a prime and consider the rational number
$$\frac{m}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$
If $p > 2$ show that $p \mid m$. [Hint: consider the function $f : \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$ defined by $f(x) = x^{-1}$.]

6. Exercise 4.21 on page 82.

7. Exercise 6.22 on page 118.