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 $PU + QV = (P, Q)$.

   Proof. We apply division with remainder as follows: $R_{-1} = P$, $R_0 = Q$, $R_{n-1} = R_n Q_{n+1} + R_{n+1}$ with $\deg R_{n+1} < \deg R_n$. We collect the results in the tabel:

$$
\begin{aligned}
P &= Q(X^2 + 2X + 2) + (3X^4 + 3X^3 + 6X^2 + X + 2) \\
Q &= (3X^4 + 3X^3 + 6X^2 + X + 2)(5X + 1) + (2X^3 + 4X + 6) \\
3X^4 + 3X^3 + 6X^2 + X + 2 &= (2X^3 + 4X + 6)(5X + 5) + 0
\end{aligned}
$$

   Recall that $R_n = PU_n + QV_n$ where

$$
\begin{aligned}
U_{n+1} &= U_{n-1} - Q_{n+1} U_n \\
V_{n+1} &= V_{n-1} - Q_{n+1} V_n
\end{aligned}
$$

   where $U_{-1} = 1$, $V_{-1} = 0$, $U_0 = 0$, $V_0 = 1$.

n	R_n	Q_n	U_n	V_n
-1	P	$-$	1	0
0	Q	$-$	0	1
1	$3X^4 + 3X^3 + 6X^2 + X + 2$	$X^2 + 2X + 2$	1	$-(X^2 + 2X + 2)$
2	$2X^3 + 4X + 6$	$5X + 1$	$2X + 6$	$5X^3 + 4X^2 + 5X + 3$

   and so

$$P \cdot U_2 + Q \cdot V_2 = 2X^3 + 4X + 6$$

   By convention the gcd of two polynomials is monic so we divide by 2 by multiplying with $4 \equiv 2^{-1} \pmod 7$ to get

   (a) $(P, Q) = X^3 + 2X + 3$ and

   (b) $P \cdot (X + 3) + Q \cdot (6X^3 + 2X^2 + 6X + 5) = (P, Q)$.

   □

2. Show that the equation

$$x^2 + y^2 + z^2 = 20152015$$

has no integral solutions. [Hint: Try congruences modulo powers of 2.]

Proof. Modulo 2 or 4 as in class we get nowhere because $x^2 \equiv 0, 1 \pmod 4$ and $x^2 + y^2 + z^2$ could take any residue mod 4. Modulo 8 though $x^2 \equiv 0, 1, 4 \pmod 8$ and so $x^2 + y^2 + z^2 \equiv 0, 1, 2, 3, 4, 5, 6 \pmod 8$ whereas $20152015 \equiv 7 \pmod 8$. □

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.]

Proof. From Euler we know that if x is coprime to 9 then $x^6 \equiv 1 \pmod 9$ and so $x^{216} \equiv 1 \pmod 9$. If x is divisible by 3 then clearly $x^{216} \equiv 0 \pmod 9$ as $3^{216} \mid x^{216}$. Thus $x^{216} + z^{216} \equiv 0, 1, 2 \pmod 9$. Therefore

$$x^{216} - y^{216} + z^{216} - t^{216} \mod 9 \in \{a + b \mod 9 | a, b \in \{0, 1, 2\}\} = \{0, 1, 2, 7, 8\}$$

and $5 \mod 9$ is not in this set. □

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.]

Proof. (a) Suppose x or y is nonzero but integral. Then $x^2, y^2 \geq 1$ and so $2x^2 + 7y^2 \geq 2$ so the equation has no integral solutions. It is clear that $(1/3, 1/3)$ is a rational solution as $2 + 7 = 9$.

(b) If n is not divisible by 3 then 3 is invertible mod n and so we could use the rational solution to produce a solution mod n. Suppose $k \equiv 3^{-1} \pmod n$. Then let's try $x = k, y = k$.

$$\begin{aligned} 2x^2 + 7y^2 &= 9k^2 \\ &= (3k)^2 \\ &\equiv 1^2 \equiv 1 \pmod n \end{aligned}$$

□

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 $f(x) = x^{-1}$.]

Proof. It's enough to do this when m and n are coprime, i.e., if m/n is written in lowest terms. Clearing denominators the RHS has the denominator $(p-1)!$ before simplification and so $n \mid (p-1)!$ which implies that n is invertible $\pmod p$. Thus we need to show that

$$\frac{m}{n} = \sum_{k=1}^{p-1} k^{-1} \equiv 0 \pmod p$$

and now each k^{-1} can be taken modulo p separately and we need to show that

$$\sum_{k \in \mathbb{Z}_p^\times} (k^{-1} \mod p) \equiv 0 \pmod p$$

Recall that in proving Fermat's little Theorem the idea was that $\{ax | x \in \mathbb{Z}_p^\times\} = \{x | x \in \mathbb{Z}_p^\times\}$ if $p \nmid a$ as multiplication by a is bijective and therefore a permutation of $\mathbb{Z}_p^\times$. Then the product of all the elements of $\mathbb{Z}_p^\times$ could be computed as the product of all the elements of either representation of $\mathbb{Z}_p^\times$. We employ the same idea here. The function $f(x) = x^{-1}$ is now bijective (it's surjective because $(x^{-1})^{-1} = x$ and since it's surjective on a finite set it's also bijective; alternatively if $x^{-1} = y^{-1}$ then immediately by inversion $x = y$ so the function is also injective) and therefore

$$\{x^{-1} | x \in \mathbb{Z}_p^\times\} = \{x | x \in \mathbb{Z}_p^\times\}$$

Taking the sum of all the elements in two ways we deduce that

$$\sum_{k \in \mathbb{Z}_p^\times} (k^{-1} \mod p) = \sum_{k \in \mathbb{Z}_p^\times} k = \frac{(p-1)p}{2} \equiv 0 \pmod p$$

as p is odd and so $(p-1)/2$ is an integer. ☐

6. Exercise 4.21 on page 82.

   Proof. Note that $p > 3$. Then Wilson gives modulo p the equalities

$$\begin{aligned} -1 &\equiv (p-1)! \\ &\equiv (p-4)!(p-3)(p-2)(p-1) \\ &\equiv (-1) \cdot (-2) \cdot (-3) \cdot (p-4)! \\ &\equiv -6(p-4)! \pmod p \end{aligned}$$

   as $p - k \equiv -k \pmod p$. Finally we deduce $6(p-4)! \equiv 1 \pmod p$. ☐

7. Exercise 6.22 on page 118.

   Proof. For the first part note that $p - 1 \equiv -1 \pmod p$ and so $(p-1)! \equiv -(p-2)! \pmod p$ which, using Wilson, yields $(p-2)! \equiv 1 \pmod p$.

   For the second part we'd get

$$-1 \equiv (p-1)! \equiv (p-3)!(p-2)(p-1) \equiv 2(p-3)! \pmod p$$

   so $(p-3)! \equiv -2^{-1} \pmod p$. But if p is odd then $(p-1)/2$ is an integer and $2 \cdot (p-1)/2 \equiv p - 1 \equiv -1 \pmod p$ and so $-2^{-1} \equiv (p-1)/2 \pmod p$. This implies the desired congruence. ☐