Math 40520 Theory of Number
Homework 8

Due Wednesday, 2015-11-18, in class

Do 5 of the following 6 problems. Please only attempt 5 because I will only grade 5.

1. Let a be a nonzero integer.

   (a) Show that there exists at least one prime p such that $\left(\dfrac{a}{p}\right) = 1$.

   (b) Show that there are infinitely many primes p such that $\left(\dfrac{a}{p}\right) = 1$.

   Proof. (a) Pick a large integer k such that $k^2a - 1 \neq 0, \pm 1$. Pick p any prime $\mid k^2a - 1$. Then $k^2a \equiv 1 \pmod{p}$ and so $\left(\dfrac{a}{p}\right) = 1$.

   (b) **First solution:** Suppose $p_1, \dots, p_k$ are all the primes such that $\left(\dfrac{a}{p}\right) = 1$. Write $N = (p_1 \cdots p_k)^2 - a$. Pick any prime $p \mid N$. If $\left(\dfrac{a}{p}\right) = -1$ it follows, as in class, that $p \mid x^2 - ay^2$ if and only if $p \mid x, y$. Indeed, otherwise $a \equiv (x/y)^2 \pmod{p}$ would be a quadratic residue. Thus $p \mid p_1 \cdots p_k$ and $p \mid 1$ which is impossible. The only remaining possibility is if $N \in \{-1, 0, 1\}$ in which case no such p exists, but then we may simply replace $N = (p_1 \cdots p_k)^2 - a$ with $N = (p_1 \cdots p_k)^{200} - a$ or some other large even exponent.

   Second solution: Look at $P(X) = aX^2 - 1$. Then the next problem shows that there are infinitely many primes p such that $p \mid P(n)$ for some n. But then $an^2 \equiv 1 \pmod{p}$ which immediately implies that a is a quadratic residue. □

2. Let $f(X) \in \mathbb{Z}[X]$ be a nonconstant polynomial. Consider $\mathcal{P} = \{p \text{ prime} \mid p \mid f(n) \text{ for some integer } n\}$. (For example when $f(0) = 0$ then every prime number is in $\mathcal{P}$.)

   (a) If $f(0) \neq 0$ show that $g(m) = f(f(0)m)/f(0)$ defines a polynomial with integer coefficients $g(X) \in \mathbb{Z}[X]$.

   (b) Show that the set $\mathcal{P}$ is always infinite. [Hint: If $\mathcal{P} = \{p_1, \dots, p_k\}$ look at a prime dividing $g(mp_1 \cdots p_k)$ for m large enough.]

   Proof. (a) Write $f(X) = a_dX^d + \cdots + a_1X + a_0$ in which case $f(0) = a_0$ and

$$g(X) = f(f(0)X)/f(0) = a_d a_0^{d-1} X^d + a_{d-1} a_0^{d-2} X^{d-1} + \cdots + a_1 X + 1 \in \mathbb{Z}[X]$$

   (b) The case $f(0) = 0$ is trivial as then $\mathcal{P}$ consists of all primes. Assuming that $f(0) \neq 0$, the set $\mathcal{P}$ is nonempty as for n large enough $f(n)$ is large so it has some prime divisor. Suppose $\mathcal{P} = \{p_1, \dots, p_k\}$

is finite. The polynomial $h(X) = g(Xp_1 \cdots p_k)$ is nonconstant and so for m large enough the value $h(m)$ is large and therefore has a prime factor p. Thus

$$p \mid 1 + \sum_{i=1}^{d} a_i a_0^{i-1} m^i (p_1 \cdots p_k)^i = f(f(0)mp_1 \cdots p_k)/f(0) \mid f(f(0)mp_1 \cdots p_k)$$

By definition this implies that $p \in \mathcal{P}$ and so $p = p_i$ for some i. But then $p \mid 1$ which is impossible. □

3. Prove explicitly, using the AKS algorithm, that 31 is a prime. Don't verify all the polynomial congruences, but compute which congruences one needs to check.

   Proof. We seek the smallest r such that the multiplicative order of 31 mod r is at least $(\log_2(31))^2 = 24.54\ldots$. The multiplicative order of n mod r is at most $\varphi(r)$ (by Euler) so our r must be such that $\varphi(r) \geq 25$ and, in particular, $r \geq 25$. The smallest r with this property is $r = 29$ and we simply note that $31 \mod 29 = 2$ has multiplicative order 28 as $2^{14} \equiv -1 \pmod{29}$. So our $r = 29$.

   Next, the bound on a is $\sqrt{\varphi(r)} \log_2(n) = 26.21\ldots$.

   Thus we need to verify the congruences

$$(X + a)^{31} \equiv X^{31} + a \pmod{31, X^{29} - 1}$$

   for $1 \leq a \leq 26$. □

4. Let m and n be two nonzero integers. Show that $a \equiv b \pmod{m, n}$ if and only if $a \equiv b \pmod{(m, n)}$.

   Proof. Let $d = (m, n)$. If $a \equiv b \pmod{m, n}$ then there exist integers u and v such that $a - b = um + vn$ and so $d \mid um + vn = a - b$ implying that $a \equiv b \pmod{d}$. Bezout implies that there exist integers p and q such that $pm + qn = d$. If $a \equiv b \pmod{d}$ then $a - b = kd$ for some integer k and so $a - b = k(pm + qn) = kpm + kqn$ so $a \equiv b \pmod{m, n}$. □

5. Show that there exists no polynomial $P(X) \in \mathbb{Z}[X]$ with the property that for any two polynomials $A(X), B(X) \in \mathbb{Z}[X]$ the following is true:

$$A(X) \equiv B(X) \pmod{2, X^2 - 1} \text{ if and only if } A(X) \equiv B(X) \pmod{P(X)}$$

   Proof. Suppose such a polynomial $P(X)$ exists. Certainly $2 \equiv 0 \pmod{2, X^2 - 1}$ and so $2 \equiv 0 \pmod{P(X)}$ implying that $P(X) \mid 2$. Thus $P(X) = 1$ or 2. Similarly $X^2 - 1 \equiv 0 \pmod{2, X^2 - 1}$ implies that $X^2 - 1 \equiv 0 \pmod{P(X)}$ and so $P(X) \mid X^2 - 1$. As $2 \nmid X^2 - 1$ ($(X^2 - 1)/2$ does not have integral coefficients) it follows that $P(X) = 1$. But then $1 \equiv 0 \pmod{P(X)}$ and so it would follows that $1 \equiv 0 \pmod{2, X^2 - 1}$ which would imply there exist two polynomials with integral coefficients $A(X)$ and $B(X)$ such that $1 = 2A(X) + (X^2 - 1)B(X)$. Plugging in $X = 1$ yields $1 = 2A(1)$ which is impossible as $A(1) \in \mathbb{Z}$. □

6. Let $L \subset \mathbb{R}^2$ be a lattice in the plane generated by two vectors $u = (a, b)$ and $v = (c, d)$. Show that the fundamental parallelogram has area $\left| \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right|$.

   Proof. From calculus, the area of the parallelogram is the length of the cross product $(a, b) \times (c, d)$ which is $\begin{vmatrix} i & j & k \\ a & b & 0 \\ c & d & 0 \end{vmatrix} = \begin{vmatrix} a & b \\ c & d \end{vmatrix} k$. □