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 $\left(\frac{a}{p}\right) = 1$.
   (b) Show that there are infinitely many primes p such that $\left(\frac{a}{p}\right) = 1$.
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.]
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.
4. Let m and n be two nonzero integers. Show that $a \equiv b \pmod{m, n}$ if and only if $a \equiv b \pmod{(m, n)}$.
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:
$$A(X) \equiv B(X) \pmod{2, X^2 - 1} \text{ if and only if } A(X) \equiv B(X) \pmod{P(X)}$$
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 $\left|\det \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right|$.