M445/845, Homework 4, due Monday, November 11, 2013

Instructions: Do any three problems.

(1) Consider the nonzero rationals, $\mathbf{Q}^*$. This is a group under multiplication.

(a) If $r \in \mathbf{Q}^*$, show that there is a unique expression of r as $\frac{m}{n}$, such that $m > 0$ and $n \neq 0$ are integers with $(m, |n|) = 1$.

(b) Show that $\mathbf{Q}^*$ is not a cyclic group. (I.e., show that there is no nonzero rational r such that every nonzero rational c is a power of r.)

(2) Let a, b, c, d be positive integers and let s be any integer. Prove that $x = s$ is a solution to $adx \equiv bd \mod cd$ if and only if $x = s$ is a solution to $ax \equiv b \mod c$.

(3) Use techniques developed in class to find all positive integer solutions $x \leq m$ for $m = 519223 = 71^2 * 103$ to the equation $x^2 \equiv 480777 \mod m$.

(4) Show how to use quadratic reciprocity in conjunction with techniques developed in class to determine whether $x^2 \equiv 85 \mod 23319936929$ has a solution. (Note: $p = 23319936929$ is known to be prime.)

(5) Let p_n denote the nth prime, so, for example, $p_1 = 2$ and $p_5 = 11$.

(a) Use induction to show that $p_n \leq 2^n$. (You may assume without proof a theorem known as Bertrand's postulate, viz., that for any positive integer n, there is a prime p with $n < p \leq 2n$.)

(b) For each positive integer n, let $\pi(n)$ be the number of primes $p \leq n$. Show that $\log_2(k) - 1 < \pi(k)$ for each positive integer k. [Hint: if $\pi(k) = n$ show that $k < 2^{n+1}$.]

(6) Let R be a Euclidean domain with Euclidean function d. For any nonempty subset $S \subseteq R$, let $(S) \subseteq R$ be the set of all R-linear combinations of elements of S; i.e., $a \in (S)$ if and only if there are elements $a_1, \ldots, a_t \in S$ and $r_1, \ldots, r_t \in R$ for some t such that $a = r_1 a_1 + \cdots + r_t a_t$. Show that there exists an element $c \in (S)$ such that $d(c) \leq d(v)$ for all $v \in (S)$, and that $(S) = cR$, where $cR = \{rc : r \in R\}$. (This shows that R is a PID, or Principal Ideal Domain.)

(7) We know that $\mathbf{Q}[x]$ is a Euclidean domain with Euclidean function deg. Show that $\mathbf{Z}[x]$ (i.e., polynomials with integer coefficients) is not a Euclidean domain. (Thus while deg is a Euclidean function for $\mathbf{Q}[x]$, it is not a Euclidean function for $\mathbf{Z}[x]$—because there isn't any!) [Hint: Show that $\mathbf{Z}[x]$ is not a PID. For example, show that $(S) = E_0$,where $S = \{2, x\}$ and E_0 is the subset of polynomials $f \in \mathbf{Z}[x]$ such that $f(0)$ is even is not of the form $c\mathbf{Z}[x]$ for any $c \in \mathbf{Z}[x]$; then apply Problem 3. You may asume without proof that $\mathbf{Z}[x]$ is a UFD.]