Math 42-Number Theory
Problem Set #7
Due Thursday, April 7, 2011

10. Prove that given natural numbers a and b, there exist integers q, r, ε such that $a = bq + \varepsilon r$ where $\varepsilon = \pm 1$ and $0 \le r \le \frac{b}{2}$. Prove in addition, that $\varepsilon = (-1)^{\lfloor \frac{2a}{b} \rfloor}$. Here, $\lfloor x \rfloor$ means the greatest integer less than or equal to x, so for example $\lfloor \frac{1}{2} \rfloor = 0$, $\lfloor 2 \rfloor = 2$ and $\lfloor \pi \rfloor = 3$. You may assume that given a and b, there are integers q' and r' such that $a = bq' + r'$ and $0 \le r' < b$.

Solution: Given a and b, we know that there are integers q' and r' such that $a = bq' + r'$ with $0 \le r' < b$. Now, if $r' < b/2$, we can let $q = q'$, $r = r'$ and $\varepsilon = +1$. Notice that in this case, $\lfloor 2a/b \rfloor = \lfloor 2q' + 2r'/b \rfloor = 2q'$ since $0 \le r' < b/2$ implies that $0 \le 2r'/b < 1$. Thus, $\varepsilon = (-1)^{\lfloor 2a/b \rfloor}$ in this case as desired.

On the other hand, if $r' \ge b/2$, we can let $q = q' + 1$, $r = b - r'$ and $\varepsilon = -1$. Notice that if $a = bq' + r'$, then $a = b(q + 1) + (-1)(b - r')$, so we do have $a = bq + \varepsilon r$. In this case, $\lfloor 2a/b \rfloor = \lfloor 2q' + 2r'/b \rfloor = 2q' + 1$ since $b/2 \le r' < b$ implies that $1 \le 2r'/b < 2$. Thus, $\varepsilon = (-1)^{\lfloor 2a/b \rfloor}$ as desired.

11. Extra Credit: Prove that there are infinitely many primes of the form $4k+1$. (Hint: Show that for any $N > 1$, there is a prime $p > N$ with $p \equiv 1 \mod 4$. Do this by setting $m = (N!)^2 + 1$ and considering the smallest prime p dividing m. Is $p > N$? Why must p be 1 mod 4?)

Solution: For any $N > 1$, we'll find a prime p such that $p > N$ and $p \equiv 1 \mod 4$. This will show that there are infinitely many primes of the form $4k+1$, since there will never be a biggest prime of the form $4k + 1$.

Consider $m = (N!)^2 + 1$, and let p be the smallest prime dividing m. Now, none of the integers $1, 2, 3, \ldots, N$ divide m, so $p > N$. We'll show that p must be $1 \mod 4$ by showing that -1 is a square mod p. In fact, $(N!)^2 \equiv -1 \mod p$, so -1 is a square mod p. Thus, we know p must be $1 \mod 4$, and we have produced a prime $p > N$ of the form $4k + 1$. Therefore, there are infinitely many primes of the form $4k + 1$.