Geoffrey Parker HW 11: 2.37, 2.38, 2.41 M328K February 28th, 2012

2.37 Theorem. If r_1, r_2, \ldots, r_m are natural numbers and each one is congruent to 1 modulo 4, then the product $r_1r_2 \cdots r_m$ is also congruent to 1 modulo 4.

Proof. Let r_1, r_2, \ldots, r_m be natural numbers with each one being congruent to 1 modulo 4. We will show that the product $r_1r_2\cdots r_m$ is also congruent to 1 modulo 4. Define a sequence of s's, with $s_0 = 1$ and every subsequent $s_i = s_{i-1}r_i$. By this definition, $s_m = r_1r_2\cdots r_m$. We will show by induction that $s_m \equiv 1 \pmod{4}$. As a base case, $s_1 = 1 \cdot r_1$, and $r_1 \equiv 1 \pmod{4}$ by definition. Our induction hypothesis is that there exists some natural number N such that $s_N \equiv 1 \pmod{4}$. Then $s_{N+1} = s_N r_{N+1}$. Since $s_N \equiv 1 \pmod{4}$ and $r_{N+1} \equiv 1 \pmod{4}$, then by theorem $1.14 \ s_N r_{N+1} \equiv 1 \cdot 1 \pmod{4}$. Therefore $s_{N+1} \equiv 1 \pmod{4}$. We have now shown by induction that $r_1 r_2 \cdots r_m$ is congruent to 1 modulo 4.

2.38 Theorem (Infinitude of 4k + 3 Primes Theorem). There are infinitely many prime numbers that are congruent to 3 modulo 4.

Proof. Let P be the set of primes numbers that are congruent to 3 modulo 4. We will show that P is infinite. Since 3 is prime and $3 \equiv 3 \pmod{4}$, P is not empty. Assume by way of contradiction that P is finite, with some cardinality n. Let the natural number Q be the product of all the primes in P. By repeatidly applying theorem 1.14, we see that $Q \equiv 3^n \pmod{4}$. Now, we have two cases, n is even and n is odd. If n is odd, then $3^n \equiv 3 \pmod{4}$, so by theorem 1.11 $Q \equiv 3 \pmod{4}$. Let q be a prime divisor of Q + 4. (TODO: $q \equiv 3 \pmod{4}$) Then we have $q \mid Q$ and $q \mid Q + 4$. Therefore $q \mid 4$, which is a contradiction because q is prime and $q \equiv 3 \pmod{4}$. Let q be a prime divisor of Q + 2. (TODO: $q \equiv 3 \pmod{4}$) Then we have $q \mid Q$ and $q \mid Q + 2$. Therefore $q \mid 2$, which is a contradiction because q is prime and $q \equiv 3 \pmod{4}$. \square

2.41 Exercise. Use polynomial long division to compute $(x^m - 1) \div (x - 1)$.

Solution.

$$x^{m} - 1 = x^{m-1}(x-1) + x^{m-1} - 1$$

$$x^{m-1} - 1 = x^{m-2}(x-1) + x^{m-2} - 1$$

$$\dots$$

$$x^{2} - 1 = x(x-1) + x - 1$$

$$x - 1 = 1(x-1)$$

Therefore:

$$(x^m - 1) \div (x - 1) = x^{m-1} + x^{m-2} + \dots + x + 1$$