Solutions to Homework 7.

March 27, 2013

Problem 42.

This requires a calculation for each $a \in \mathbb{Z}_{13} - \{0\}$.

For example, this is the result for $a = 6$.

The functional digraph for multiplication by 6 is

$$0 \to 0$$

$$1 \to 6 \to 10 \to 8 \to 9$$

$$\to 2 \to 12 \to 7 \to 3 \to 5 \to 4 \to 11 \to 1.$$

The order k is the length of the loop starting from 1, in this case 12.

Problem 44.

We can check that 341 is not prime using Fermat's Little Theorem. For, if it were prime, then $7^{340} \equiv 1 \bmod 341$. But the calculation at the top of page 149 in the book shows that $7^{340} \equiv 56 \bmod 341$.

To contradict Fermat's conjecture we need to show that $2^{341} = 2 \bmod 341$.

We compute in $\mathbb{Z}_{341}$,

$$2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 16, 2^5 \equiv 32, 2^6 \equiv 64, 2^7 \equiv 128,$$

$$2^8 \equiv 256, 2^9 \equiv 512 \equiv 171, 2^{10} \equiv 342 \equiv 1.$$

Hence $2^{341} \equiv 2^{34 \cdot 10+1} \equiv 2 \bmod 341$ as required.

Problem 45.

Let m be a positive integer and $m = p_1^{k_1} \dots p_N^{k_N}$ be its prime factorization. Let

$$f(x) = (x^{p_1} - x)^{k_1} \dots (x^{p_N} - x)^{k_N}.$$

This is a polynomial with leading coefficient 1.

Then by Fermat's Little Theorem $(x^{p_1} - x)$ is divisible by p_1 for all $x \in \mathbb{Z}$. Therefore $(x^{p_1} - x)^{k_1}$ is divisible by $p_1^{k_1}$. Similarly the ith factor is divisible by $p_i^{k_i}$ and the polynomial $f(x)$ is divisible by $p_1^{k_1} \ldots p_N^{k_N}$ for all $x \in \mathbb{Z}$. Hence $f(x) \equiv 0 \bmod m$ for all x.

Alternatively Fermat's theorem can be avoided by just setting

$$f(x) = x(x+1)(x+2)\ldots(x+m-1).$$

Then for any $x \in \mathbb{Z}$, $f(x)$ is a product of m consecutive integers. One of these integers must be divisible by m and so $f(x)$ is divisible by m. (This is simpler but the polynomial typically will have higher degree.)

Problem 47.

By Fermat's Little Theorem we know that $(p-1)! \equiv -1 \bmod p$. If p is an odd prime then $p > 2$, or $p \geq 3$ and so we can write the identity as

$$(p-3)!(p-2)(p-1) \equiv -1 \bmod p.$$

Now, $(p-2)(p-1) = p^2 - 3p + 2 \equiv 2 \bmod p$. Hence the identity becomes $2(p-3)! \equiv -1 \bmod p$ as required.

Problem 48.

We prove by contrapositive. Suppose that p is not prime. Our goal is to show that $(p-1)! \not\equiv -1 \text{mod} p$. As p is not prime we can write $p = ab$ for some divisors a, b with $2 \leq a, b \leq p-1$. If $a \neq b$ then $ab|(p-1)!$ since both numbers appear as separate factors in the factorial. Therefore $(p-1)! \equiv 0 \bmod p$.

In the second case we suppose that $a = b$ and $p = a^2$. Further suppose that $a > 2$. Then $p = a^2 > 2a$ and a and $2a$ appear as separate factors in $(p-1)!$ and again $(p-1)! \equiv 0 \bmod p$.

Finally we suppose that $p = 2^2 = 4$. Then $(p-1)! = 3! \equiv 2 \bmod 4$.

In conclusion, if p is not prime then either $(p-1)! \equiv 0 \bmod p$ or $p = 4$ and $(p-1)! \equiv 2 \bmod p$. In both cases $(p-1)!$ is not congruent to -1 and so the proof is complete.