Foundations Homework 6

TJ Liggett

10 October 2019

Chapter Two

Assignment 14 *Prove Fermat's Little Theorem: If n is any natural number, and p any prime, then $n^p \equiv n \pmod{p}$.*

Base case: Let $n = 1$, and p be any prime. Since $1^p = 1$ for any prime, and $1 \equiv 1 \pmod{p}$, this is trivial.

Inductive hypothesis: For some natural number k and any prime p, $k^p \equiv k \pmod{p}$.

Consider the $n + 1$ case. By the binomial theorem, it follows that:

$$(n+1)^p = \sum_{j=0}^{p} \binom{p}{j} n^{p-j} \cdot 1^j$$

$$= \binom{p}{0} n^p + \binom{p}{1} n^{p-1} \cdot 1 + \binom{p}{2} n^{p-2} \cdot 1^2 + \cdots + \binom{p}{p-1} n^{p-(p-1)} \cdot 1^{p-1} + \binom{p}{p} \cdot 1^p$$

We can simplify the trivial combinations $\binom{p}{0} n^p$, $\binom{p}{p} = 1$, as well as multiplication by 1, to obtain:

$$= n^p + \binom{p}{1} n^{p-1} + \binom{p}{2} n^{p-2} + \cdots + \binom{p}{p-1} n + 1$$

Observe that for any combination where p is prime and $0 < j < p$, it is true that $p | \binom{p}{j}$. By the definition of divides, we can infer that for some natural number s,

$$n^p + \binom{p}{1} n^{p-1} + \binom{p}{2} n^{p-2} + \cdots + \binom{p}{p-1} n + 1$$

$$= n^p + sp + 1$$

By the inductive hypothesis, $n^p \equiv n \pmod{p}$. By the definition of modular division, it follows that

$$n^p = q_1 p + r, n = q_2 p + r$$

For some natural numbers q_1, q_2, r where $r < p$. Observe that

$$n^p + sp + 1 = q_1 p + r + sp + 1 = (q_1 + s)p + r + 1$$

$$n + 1 = q_2 p + r + 1$$

Consider two cases, one in which $r + 1 < p$, and one in which $r + 1 = p$.

1. If $r+1 < p$, then because natural numbers are closed under addition, $(q_1+s), q_2$ are natural numbers, it follows $(n+1)^p \equiv n+1 \pmod{p}$ with a remainder of $r+1$.
2. If $r + 1 = p$, then it follows that $p|(n+1)^p, n+1$ and that $(n+1)^p \equiv n+1 \pmod{p}$

Therefore, by induction, if n is any natural number, and p any prime, then $n^p \equiv n \pmod{p}$.

Exercise 15 *Use Euclid's algorithm to compute (36,100), (306,378), and (588, 1575).*

For (36, 100), $m = 36, n = 100$

$$100 = 36 * 2 + 28$$
$$36 = 28 * 1 + 8$$
$$28 = 8 * 3 + 4$$
$$8 = 4 * 2 + 0$$
$$(36, 100) = 4$$

For (306, 378), $m = 306, n = 378$

$$378 = 306 * 1 + 72$$
$$306 = 72 * 4 + 18$$
$$72 = 18 * 4 + 0$$
$$(306, 378) = 18$$

For (588, 1575), $m = 588, n = 1575$

$$1575 = 588 * 2 + 399$$
$$588 = 399 * 1 + 189$$
$$399 = 189 * 2 + 21$$
$$189 = 9 * 21$$
$$(588, 1575) = 21$$

Assignment 16 *Prove that the last positive remainder in the sequence generated from $m > n$ by the Euclidean Algorithm is $g = (m, n)$.*

Assume, without loss of generality, $m < n$. Then using the Euclidean Algorithm, we may write

$$n = q_1 m + r_1$$
$$m = q_2 r_1 + r_2$$
$$r_1 = q_3 r_2 + r_3$$
$$\cdots$$
$$r_{t-1} = q_{t+1} r_t + r_{t+1}$$
$$r_t = q_{t+2} r_{t+1}$$

where $m > r_1 > r_2 > \cdots > r_{t+1} > 0$. Clearly $r_{t+1} | r_t$. Therefore,

$$\begin{aligned} r_{t+1} &= q_{t+1}(q_{t+2} r_{t+1}) + r_{t+1} \\ &= (q_{t+1} q_{t+2} + 1) r_{t+1} \end{aligned}$$

showing that $r_{t+1} | r_{t-1}$. Using the same process, we can show that r_{t+1} is a divisor of $r_{t-2}, \ldots, r_1, m, n$. Since $r_{t+1} | m, n$, $r_{t+1} | g$, the greatest common divisor of m and n. Observe that since $g | m, n$ and $n = q_1 m + r_1$, then

$$xg = q_1 yg + r_1$$
$$r_1 = (q_1 y - x) g$$

And thus $g | r_1$. By similar logic, it follows that $g | r_2, r_3, \ldots, r_t, r_{t+1}$. Because $r_{t+1} | g$ and $g | r_{t+1}$, $r_{t+1} = g$, and is the greatest common divisor of m, n.

Therefore, the last positive remainder in the sequence generated from $m > n$ by the Euclidean Algorithm is $g = (m, n)$.

Exercise 18 *Make addition and multiplication tables for the remainders upon division by $m = 6$. Which of the remainders 0,1,2,3,4,5 has a multiplicative inverse?*

Addition table for $m = 6$:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Multiplication table for $m = 6$:

x	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

1 and 5 have a multiplicative inverse of themselves.

Exercise 19 *Repeat the preceding exercise for $m = 2, 3, 4, 5, 8$. For what values of m do all the non-zero remainders upon division by m have multiplicative inverses?*

Addition table for $m = 2$:

+	0	1
0	0	1
1	1	0

Multiplication table for $m = 2$:

x	0	1
0	0	0
1	0	1

Addition table for $m = 3$:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Multiplication table for $m = 3$:

x	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Addition table for $m = 4$:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Multiplication table for $m = 4$:

x	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Addition table for $m = 5$:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Multiplication table for $m = 5$:

x	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Addition table for $m = 8$:

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Multiplication table for $m = 8$:

x	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

When values of m are prime, all the non-zero remainders upon division by m have multiplicative inverses.

Assignment 20 *Prove that if and only if m is prime, the remainders $r = 1, \ldots, m-1$ satisfy the eighth field axiom. That is, when m is prime each $r = 1, \ldots, m-1$ has a multiplicative inverse modulo m; however, if m is composite, this is not the case.*

First, assume m is prime. Then, as prime numbers are only divisible by 1 and themselves, for every natural number $r = 1, \ldots, m-1$, it follows that $\gcd(m, r) = 1$. By Theorem 2.8, it can be said that $m \cdot x + r \cdot y = 1$, where x, y are whole numbers. Thus, $mx = 1 - ry, m(-x) = ry - 1$, and so $m|(ry - 1)$. From this we can infer that $ry \equiv 1 \pmod{m}$. Since the natural numbers are closed under multiplication, we can be certain that y is a natural number less than m. Hence, r has a multiplicative inverse such that $r \cdot y = 1$. Hence, if m is prime, each $r = 1, \ldots, m-1$ has a multiplicative inverse modulo m.

Second, assume that for a natural number m, each $r = 1, \ldots, m-1$ has a multiplicative inverse modulo m. By way of contradiction, assume m is composite.

Then there exists a natural number $1 < n < m$ where $n|m$. Since $n > 1$, it follows that $n \nmid 1$. Thus, $n \nmid (mx + 1)$ for any natural number x, and as such $nx \not\equiv 1 \pmod{m}$, and n has no multiplicative inverse. This is a contradiction, so if for a natural number m, each $r = 1, \ldots, m - 1$ has a multiplicative inverse modulo m, then m is prime.

Therefore, if and only if m is prime, the remainders $r = 1, \ldots, m - 1$ satisfy the eighth field axiom.