Number Theory
(Summer Project - 2016)
Indian Statistical Institute, Bangalore

Shubhangi Ghosh
EE15B129
Department of Electrical Engineering

December 21, 2017

1 INTRODUCTION:

This report presents the study of some theorems and problems based on some concepts of Number Theory.

2 Theorem 1 - Fermat's Little Theorem

2.1 Proof By Induction

For any integer a, and a prime number, p:

$$a^p \equiv a\,(mod\,p)$$

2.1.1 Proof:

$$1^p \equiv 1\,(mod\,p)$$

Let

$$n^p \equiv n\,(mod\,p)$$

To prove,

$$(n+1)^p \equiv (n+1)\,(mod\,p)$$

$$1 + \begin{pmatrix} p \\ 1 \end{pmatrix} n + ... \begin{pmatrix} p \\ p-1 \end{pmatrix} n^{p-1} + \begin{pmatrix} p \\ p \end{pmatrix} n^p - n - 1 \equiv 0\,(mod\,p)$$

$since \begin{pmatrix} p \\ p \end{pmatrix} = 1$and $n^p \equiv n\,(mod\,p)$ and $p| \begin{pmatrix} p \\ r \end{pmatrix}\ \forall\, r \neq 0, p$, *because*
$p|p(p-1)...(p-r+1)$ and $p \nmid r!$.

2.1.2 Pseudoprimes:

$x| \begin{pmatrix} x \\ r \end{pmatrix}\ \forall\, r \neq 0, x$, when x is not prime.

2.2 Another form:

$a^{p-1} \equiv 1\,(mod\,p)$ p is prime and $p \nmid a$.

3 Theorem 2- Wilson's Theorem

$(p-1)! \equiv -1\,(mod\,p)$, when p is prime.

3.1 Proof

$(p-1)! \equiv (p-1)\,(mod\,p)$
1.2.3...$(p-1) \equiv (p-1)\,(mod\,p)$
This is because for every $a\,\epsilon\,[2, p-2]$, there exists a b s.t. $ab \equiv 1\,(mod\,p)$.
$ab - 1 = pk$
$ab - pk = 1$.This is true since $(a, p) = 1$, $since\,p$ is a prime.
Also, $b \neq a$, since if $b = a$, $a^2 \equiv 1\,(mod\,p)$, $a^2 - 1 \equiv 0\,(mod\,p)$, $(a-1)(a+1) \equiv 0\,(mod\,p)$, a=1 or a=p-1
Thus, the numbers $a \in [2, p-2]$, can be paired.

4 Theorem 3 - Chinese Remainder Theorem

4.1 Theorem:

Let $m_1, m_2...m_r$ exists s.t. $(m_i, m_j) = 1\,\forall\,i \neq j$, then there exists a unique x s.t.

$$x \equiv c_1\,(mod\,m_1)$$
$$x \equiv c_2\,(mod\,m_2)$$
$$...$$
$$x \equiv c_r\,(mod\,m_r)$$

4.2 Proof:

4.2.1 For two modulo equations:

Let there exist x s.t. $x \equiv c_1\,(mod\,m_1)$ and $x \equiv c_2\,(mod\,m_2)$.
This implies $x = c_1 + k_1m_1 = c_2 + k_2m_2$.
$$k_1m_1 - k_2m_2 = c_1 - c_2.$$
Such a pair of (k_1, k_2) exists because $(m_1, m_2) = 1$.

4.2.2 Multiple Modulo Equations:

$x = c_1 + k_1m_1 = c_2 + k_2m_2 = ...c_r + k_rm_r$.
$(m_i, m_j) = 1$ implies $\exists\,(k_i, k_j)\,s.t.\,c_i + k_im_i = c_j + k_jm_j\,\forall\,i \neq j$.

4.3 Algorithm to find x

4.3.1 For two modulo equations:

Let,

$$x \equiv c_1\,(mod\,m_1)$$
$$x \equiv c_2\,(mod\,m_2)$$

$(m_1, m_2) = 1$ implies $\exists\,(m_1^{'}, m_2^{'})\,s.t.$

$$m_1m_1^{'} \equiv 1\,(mod\,m_2)$$
$$m_2m_2^{'} \equiv 1\,(mod\,m_1)$$

Then,

$$x = c_2m_1m_1^{'} + c_1m_2m_2^{'}$$

4.3.2 Multiple Modulo Equations:

Let,

$$x \equiv c_1 \,(mod\, m_1)$$
$$x \equiv c_2 \,(mod\, m_2)$$
$$...$$
$$x \equiv c_r \,(mod\, m_r)$$

$(m_i, \prod_j m_j) = 1$
Let, $\prod_i m_i = n_i$. This implies, $(m_i, n_i) = 1, \implies \exists\, n_1^{'}\, s.t.\ n_1 n_1^{'} \equiv 1 \,(mod\, m_1)\ \forall\, i \in [1, r]$.
Thus,

$$x = \sum_{i=1}^{r} c_i n_i n_i^{'}$$

5 Fundamental Divisibility Axioms:

$$a|b \implies a|bc \forall\, c \epsilon Z$$
$$a|b\, and\, b|c \implies a|c$$

$$a|b\, and\, a|c \implies a|(bx + cy)$$

$$a|b\, and\, b|a \implies a = \pm b$$
$$a > 0, b > 0 \implies a \leq b$$
$$m \neq 0, a|b \implies ma|mb$$

6 Division Algorithm:

$b = aq + r \qquad 0 \leq r < a$

6.1 Proof:

Let us consider,

$$...b - 2a, b - a, b, b + a, b + 2a...$$

r is the smallest number in the above series as it satisfies the equality and the inequality in the theorem statement.
To prove uniqueness,
Let q_1, r_1 exist s.t. they satisfy the constraints of the theorem.
We prove that $r_1 = r$ by contradiction.
Let $r_1 \neq r$, then $r_1 > r$ since r is the smallest number which satisfies the given constraints.
Also, $0 < r_1 - r < a$, as $r < a$, $r_1 < a$.
$r_1 - r = a(q - q_1), \implies a \leq (r_1 - r)$. This is a contradiction.

7 Problems:

7.1 Problem 1:

If $g = (b, c)\, \exists\, x_0, y_0\, s.t.\, q = bx_0 + cy_0$.

7.2 Answer:

Let l be the least number s.t. $l = bx + cy$. Let's assume $l \nmid b$. $l = bq + r$, $0 < r < b$. $\implies r = bq - l$.
$\implies r = bq - bx - cy \implies r = b(q - x) - cy$. But $r < l$. This is a contradiction.
$\therefore l|b$ and $l|c$.
To prove l is the g.c.d.,
$b = gB$ and $c = gC \implies l = gBx + gCy$
$\therefore g|l \implies g \leq l$
$g < l$ is impossible, $\because g$is the greatest common divider.
$\therefore g = l$.
Basically all factors must be there.

7.3 Definition:

7.3.1 Fermat's numbers:

$2^{2^n} + 1$.
If $2^k + 1$ is prime, $k = 2^n$.
$\because (x + 1)|(x^k + 1)$ if k is odd.

But not all Fermat's number are prime, since the converse may not be true.

7.4 Problem 2:

$(n - 1)^2|(n^k - 1)$ iff $(n - 1)|k$.

7.4.1 Solution:

$$n^k - 1 = (((n-1)+1)^k - 1) = (n-1)^k + \begin{pmatrix} k \\ 1 \end{pmatrix}(n-1)^{k-1} + ... \begin{pmatrix} k \\ k-2 \end{pmatrix}(n-1)^2 + k(n-1).$$

Only the last term doesn't have $(n - 1)^2$.

7.5 Problem 3:

$\exists\ x\ s.t.\ ax \equiv 1(mod\, m)\ \ iff\ \ (a, m) = 1$.

7.5.1 Solution:

$$ax - 1 = km$$
$$ax - km = 1\ iff\ (a, m) = 1$$

8 Euler's Theorem:

$$a^{\phi(m)} \equiv 1(mod\, m)\, if\, (a, m) = 1.$$

$\phi(m)$ is the reduced residue class of m.

8.1 Complete Residue Class:

All modulo classes s.t. every natural number falls into one of them, *i.e.* all possible remainders or equivalents.

8.2 Reduced Residue Class:

No.s $a_1, a_2...a_{\phi(m)}$ s.t. $a_i \not\equiv a_j \forall i \neq j$ and $(a_i, m) = 1 \forall i$.

8.3 Proof:

Let $r_1, r_2 ... r_{\phi(m)}$ be a reduced residue class of m.
Then even $ar_1, ar_2 ... ar_{\phi(m)}$ is a also a reduced residue class of m, if $(a, m) = 1.$, with a one-one direct mapping.
$\prod_{i=1}^{\phi(m)} ar_i \equiv \prod_{i=1}^{\phi(m)} r_i \, (mod\, m)$
$a^{\phi(m)} \equiv 1 (mod\, m)$
Fermat's theorem is a corollary of Euler's theorem.

9 CONCLUSION:

Number theory theorems for finding solutions to congruences have been studied and some problems have been solved based on them. This reading assignment involved studying theorems such as Fermat's theorem, Wilson's theorem, Euler's theorem, Chinese Remainder Theorem, Euclidean Algorithm and other divisibility theorems. The book that has been used for reference and problem solving during the course of this reading assignment is An Introduction to the Theory of Numbers - Niven, Zuckerman and Montgomery.