2003 Winter Camp

Number Theory Exercises

1) a) Use Inclusion/Exclusion to show directly that $\Phi(A \cdot B) = \Phi(A) \cdot \Phi(B)$ for A & B relatively prime.

   b) List all numbers $\le p^r$ which are not relatively prime to p^r, for p prime, and hence develope a formula for $\Phi(p^r)$

   c) Combine (a) and (b) for another proof of the formula for $\Phi(N)$.

2) Show that $|S_b| = p$ from the proof of Euler's Theorem.

3) Show that $S_b \cap S_c \ne \{\}$ $\Rightarrow$ $S_b = S_c$ from the proof of Euler.

4) If $f(x) = x^4 - 8x^3 + 28x^2 - 53x + 42$ and $g(x) = x^3 - 13x^2 + 46x - 48$ find the greatest common divisor of $f(x)$ and $g(x)$, and write it as a linear combination of $f(x)$ and $g(x)$. [Use Euclid's algorithm.]

5) a) Find $(N-1)!$ mod N for N composite.

   b)* A better generalization of Wilson's Theorem is $\left(\prod_{\substack{(a,N)=1 \\ a<N}} a\right) \bmod N$. What is this value?

6) For the Public Key (102, 21) a message was encrypted as 19. Calculate the Private Key and decode the message.

7) Given a full Public Key Code (N, d, e) write a formula for the factors of N in terms of N, d, and e.

8) Prove the Public Key Theorem.

9) While playing with my new bicycle lock combination (four digits each from 0 to 9), I calculated the 2003rd power of the combination. But I only remember the last four digits: 2003. What is my combination?

10) Prove the other corollaries of Euler's Theorem.

11) Find the smallest denominator for which the repeating decimal form has a repeating block of length 7.

12) Find the smallest integer, N, for which the fraction, $\frac{1}{N}$, expanded as a repeating decimal in <u>some</u> base-b has a repeating block of length 7. What is the smallest base-b for this value of N?

Wilson's Theorem: For p prime: $(p-1)! \equiv -1 \mod p$

Proof:

First examine elements which are their own multiplicative inverses mod p:

$x \cdot x \equiv 1 \mod p \Rightarrow x^2 - 1 \equiv 0 \mod p \Rightarrow (x-1)(x+1) \equiv 0 \mod p \Rightarrow x-1 \equiv 0$ or $x+1 \equiv 0 \mod p$ (prime!) $\Rightarrow x \equiv \pm 1 \mod p$.

Thus all the factors of $(p-1)!$, except 1 and $(p-1)$, can be paired with their inverses.

Theorem: (Public Key)

If $N = p \cdot q$ for distinct primes p and q,
and positive integers d and e satisfy $d \cdot e \equiv 1 \mod \Phi(N)$
Then $(m^e)^d \equiv m \mod N$ for all integers m.

Proof: Left as an exercise.

Note: For any d relatively prime to $\Phi(N)$, there exists a suitable e.

Definition: The triplet (N, d, e) describes a Public Key Code with the Public Encryption Key (N, e) and the Private Decryption Key (N, d).
A "message" is a number $m < N$ and the encrypted messege is: $m^e \mod N$.

Note: Computing d from N and e is equivalent to factoring N, and factoring is thought to be hard. So the code is secure as N is difficult to factor.

Other Corollaries of Euler's Theorem:

Repunits: If N is relatively prime to 30 then N divides some repunit (a number of the form $111\cdots1$) and the number of digits in the smallest such repunit divide $\Phi(N)$.

Repeating Decimals: If N is the denominator of a rational α, then the number of digits in the repeating part of the repeating decimal representation of α divides $\Phi(N)$.

Complex Roots of Unity: The number of primitive N^{th} roots of one ($z^N = 1$ and no smaller power of z equals 1) is exactly $\Phi(N)$.

Some Number Theory & Public Key Codes

Definition: Euler's Totient Function

$\Phi(N) = \left|\{a \in \mathbb{Z}^+ \mid a < N \text{ and } (a,N) = 1\}\right|$

= the number of positive integers less than N and relatively prime to N

Formula: (By the INCLUSION/EXCLUSION principle)

$$\Phi(N) = N - \sum_{\substack{p|N \\ \text{prime}}} \frac{N}{p} + \sum_{\substack{p \neq q|N \\ \text{prime}}} \frac{N}{p \cdot q} - \cdots \pm \frac{N}{\prod_{\substack{p|N \\ \text{prime}}} p} = N \cdot \prod_{\substack{p|N \\ \text{prime}}} \left(1 - \frac{1}{p}\right) = \prod_{\substack{p|N \\ \text{prime}}} (p-1)p^{r_p - 1} \quad \text{where } N = \prod_{\substack{p \\ \text{prime}}} p^{r_p}$$

Since $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots \pm \binom{n}{n} = \begin{cases} 0, & n > 0 \\ 1, & n = 0 \end{cases}$ $\quad n$ = # distinct prime divisors of (a, N)

Definition: The order of a number mod N.

$Ord_N(a) = Min\{p \in \mathbb{Z}^+ \mid a^p \equiv 1 \bmod N\}$

Note: Since the integers are "well-ordered", if the set is non-empty then $Ord_N(a)$ exists and $a^{Ord_N(a)} \equiv 1 \bmod N$.

Theorem: (Euler)

If a is relatively prime to N, then $\boxed{a^{\Phi(N)} \equiv 1 \bmod N.}$

Furthermore $Ord_N(a)$ divides $\Phi(N)$.

Proof:

Consider $\{a^1, a^2, a^3, \ldots, a^{\Phi(N)+1}\}$ which are all relatively prime to N.

By the Pigeonhole principle, some two of these are congruent mod N.

Say $a^m \equiv a^k \bmod N$ with $m > k$.

Then, rearranging: $a^k(a^{m-k} - 1) \equiv 0 \bmod N \Rightarrow a^{m-k} \equiv 1 \bmod N$ since $(a^k, N) = 1$.

So $p = Ord_N(a)$ exists.

For each b relatively prime to N, Let $S_b = \{ba^1 \bmod N, ba^2 \bmod N, \ldots, ba^p \bmod N\}$

Now $|S_b| = p$ for all b relatively prime to N (Exercise)

and if $S_b \cap S_c \neq \{\}$ then $S_b = S_c$. (Exercise)

So these sets partition the integers relatively prime to N and less than N.

Thus $p \mid \Phi(N)$. Say $\Phi(N) = p \cdot k$. Then $a^{\Phi(N)} = (a^p)^k \equiv 1^k = 1 \bmod N$.

Corollary: (Fermat's Little Theorem)

If p is prime, then $a^p \equiv a \bmod p$ for all integers a.

Note: If $(a, N) = 1$, then a has a multiplicative inverse mod N, namely $a^{\Phi(N)-1}$.

However this inverse is usually more easily calculated with Euclid's algorithm.