CS-2214 - ASN 2 - Ian Bormick - 250 950449

Date

1. p is prime
a is an int where a ≠ p

There exists b such that
$$ab \equiv 1 \pmod{p}$$

if a, p are relatively prime ints and $p > 1$ by Bezouts Identity

$$ba + mp = 1$$

This implies $ba + mp \equiv 1 \pmod{p}$
but because $mp \equiv 0 \pmod{p}$ it follows

$$ba \equiv 1 \pmod{p}$$

∴ b is the inverse of a modulo p

∴ Since a, b, p are arbitary (a, p relatively prime) we can conclude that every non-zero $\mathbb{Z}_p$ has a multiplicative inverse

Date

2. $x_1 \equiv 3 \pmod 5$
$x_2 \equiv 7 \pmod{12}$
$x_3 \equiv 8 \pmod{13}$

$\gcd(12,5) = 1$
$12 = 2 \cdot 5 + 2$
$5 = 2 \cdot 2 + 1$
$2 = 2 \cdot \underline{1}$

$\gcd(13,5) = 1$
$13 = 5 \cdot 2 + 3$
$5 = 3 \cdot 1 + 2$
$3 = 2 \cdot 1 + 1$
$2 = \underline{1} \cdot 2$

$\gcd(13,12) = 1$
$13 = 12 \cdot 1 + 1$
$12 = \underline{1} \cdot 12$

$x = \sum_{i=1}^{3} b_i N_i X_i \qquad N_i = \frac{N}{N_i} \qquad N = 468$

| $b_i$ | $N_i$ | $X_i$ | $b_i N_i X_i$ |
|---|---|---|---|
| 3 | 156 | 1 | $3 \cdot 156 \cdot 1 = 468$ |
| 7 | 65 | 5 | $7 \cdot 65 \cdot 5 = 2275$ |
| 8 | 60 | 5 | $8 \cdot 60 \cdot 5 = 2400$ |

$156x_1 \equiv 1 \pmod 5$
$x_1 \equiv 1 \pmod 5$

$60x_3 \equiv 1 \pmod{13}$
$8x_3 \equiv 1 \pmod{13}$
$x_3 \equiv 5 \pmod{13}$

$65x_2 \equiv 1 \pmod{12}$
$5x_2 \equiv 1 \pmod{12}$
$x_2 \equiv 5 \pmod{12}$

Page

Date

2cont) $x = \sum_{i=1}^{3} b_i N_i x_i = 468 + 2275 + 2400$

$\equiv 5143$

$x \equiv 5143 \pmod{780}$

$x \equiv 463 \pmod{780}$

∴ The remainder of x divides by 780 is <u>463</u>

3. $2^n - 1$ is prime then so is n

Proof by contradiction $\neg q \rightarrow \neg p$

Prove n is composite then so is $2^n - 1$

let $n = rs$ where $r, s > 1$ $s < n$

$2^n - 1 = 2^{rs} - 1 = (x^s - 1)(x^{s(r-1)} + x^{s(r-2)} + \cdots + x^s + 1)$

So if n is composite (rs with $1 < s < n$) then $2^n - 1$ is also composite as it is divisable by $2^s - 1$

∴ by contraposition if $2^n - 1$ is prime so is n ∎

Date

4. if possible we need to assume
$p(n) = n^2 + an + b$ is prime

$p(b) = b^2 + ab + b$ is prime
$= b(b + a + 1)$ is prime

$b = 1$

substitute in b value to get

$p(n) = n^2 + an + 1$

Similarly $p(n_0) = q$ a prime num then
$\forall t \in N \quad p(n_0 + tq)$

$= (n_0 + tq)^2 + a(n_0 + tq) + 1$
$= (n_0^2 + an_0 + 1) + q(2n_0t + t^2q + at)$
$= q(2n_0t + t^2q + at + 1)$

$\therefore$ this states that $p(n_0 + tq)$ is not a prime