CPSC 202 PSET 7

CPSC 202 student

11/1/17 5pm

A.7.1 Divisibility

Show that $\forall n \in \mathbb{N} : 12|(n(n+1)(n+2)(n+3))$

a. If $\forall n \in \mathbb{N} : 12|(n(n+1)(n+2)(n+3))$ then we can say $\forall n \in \mathbb{Z}_{12} : n(n+1)(n+2)(n+3) = 0 \pmod{12}$

b. 12 is divisible by 3 and 4.
Because 3 and 4 are relatively prime, by the Chinese Remainder Theorem:
$n(n+1)(n+2)(n+3) = 0 \pmod{12} \iff n(n+1)(n+2)(n+3) = 0 \pmod{3}$ and $n(n+1)(n+2)(n+3) = 0 \pmod{4}$.

c. In $\mathbb{Z}_3, n = 0, n = 1, n = 2$

- $n = 0 : 0(0+1)(0+2)(0+3) = 0 \pmod{3}$
- $n = 1 : 1(1+1)(1+2)(1+3) = 1(2)(3)(4)$ and in $\mathbb{Z}_3$, $1(2)(0)(1) = 0 \pmod{3}$
- $n = 2 : 2(2+1)(2+2)(2+3) = 2(3)(4)(5)$ and in $\mathbb{Z}_3$, $2(0)(1)(2) = 0 \pmod{3}$

d. In $\mathbb{Z}_4, n = 0, n = 1, n = 2, n = 3$

- $n = 0 : 0(0+1)(0+2)(0+3) = 0 \pmod{3}$
- $n = 1 : 1(1+1)(1+2)(1+3) = 1(2)(3)(4)$ and in $\mathbb{Z}_3, 1(2)(3)(0) = 0 \pmod{4}$
- $n = 2 : 2(2+1)(2+2)(2+3) = 2(3)(4)(5)$ and in $\mathbb{Z}_3, 2(3)(0)(1) = 0 \pmod{4}$
- $n = 3 : 3(3+1)(3+2)(3+3) = 3(4)(5)(6)$ and in $\mathbb{Z}_3, 3(0)(1)(2) = 0 \pmod{4}$

A.7.2 Squares

Let p be prime. Show that if $x^2 = y^2 \pmod{\text{p}}$ then either $x = y \pmod{\text{p}}$ or $x = -y \pmod{\text{p}}$

a. Subtract y^2 from both sides: $x^2 - y^2 = 0 \pmod{\text{p}}$

b. In mod p, $p|x^2 - y^2$ and after factoring, $p|(x-y)(x+y)$ since p is prime.

c. In the case that $p|x - y$, $x - y = 0 \pmod{\text{p}}$, and $x = y \pmod{\text{p}}$

d. In the case that $p|x + y$, $x + y = 0 \pmod{\text{p}}$, and $x = -y \pmod{\text{p}}$

e. Therefore, the statement is true.

A.7.3 A Series of Unfortunate Exponents

If x_0 and k are both odd, then $x_{2b^2} = x_0$

a. $x_{i+1} = x_i^k$ is equivalent to

$$x_n = \begin{cases} x_0, n = 0 \\ x_{n-1}^k, n > 0 \end{cases}$$

b. A general equation for x_n: $x_n = x_{n-1}^k = x_0^{k^n}$
Proof that $x_n = x_0^{k^n}$ by induction on n.
- Base case: $n = 0 : x_n = x_0$ and $x_0^{k^n} = x_0^{k^0} = x_0$. Therefore, $x_n = x_0^{k^n}$ when $n = 0$
- Induction step: $x_n = x_0^{k^n} \rightarrow x_{n+1} = x_0^{k^{n+1}}$
  - $x_0^{k^{n+1}} = x_0^{k \cdot k^n} = (x_0^{k^n})^k$
  - $x_{n+1} = x_n^k$ since $n > 0$.
  - For $x_n^k = (x_0^{k^n})^k$, take the k root: $x_n = x_0^{k^n}$

c. $n = 2^{b-2} : x_{2^{b-2}} = x_0^{k^{2^{b-2}}} = x_0 \pmod{2^b}$ if x_0 and k are odd.

d. Euler's theorem: $x^{\phi(m)} \pmod{\text{m}} = 1$ if gcd(x, m) = 1

e. Want: $x_0^{k^{2^{b-2}}} = C^{\phi(2^b)} x_0 = C^{2^{b-1}} x_0 = x_0 \pmod{2^b}$

f. $x^{k^{b-2}} = C^{\phi(2b)} x_0 = x_0 \pmod{2^b}$
$\phi(2^b) = (2-1)(2^{b-1}) = 2^{b-1}$
$\phi(2^{b-1}) = 2^{b-2}$
$k^{2^{b-2}} \bmod(2^{b-2}) = 1$
$k^{2^{b-2}} = q2^{b-1} + 1$

g. $x_0 = x_0^{q \cdot 2^{b-1}+1} = x_0 \cdot x_0^{q \cdot 2^{b-1}} = x_0 \cdot (x_0^q)^{2^{b-1}} \pmod{2^b}$
$= x_0 (x_0^q)^{\phi(2^b)} \pmod{2^b}$
$= x_0(1) = x_0 \pmod{2^b}$