PRIMATDIS 2 1

2 2 0 6 0 2 8 9 3 2
ALDEN LUTHFI

(a.)

1. $(1277)_8 = 1 \times 8^3 + 2 \times 8^2 + 7 \times 8^1 + 7 \times 8^0$

$= 512 + 128 + 56 + 7$

$= (703)_{10}$

$= 7 \times 10^2 + 0 \times 10^1 + 3 \times 10^0$

(b.) $(326)_{10} = 256 + + 64 + 4 + 2$

$= (1\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 0)_2$

$22 \bmod 102 = 22$

$22^2 \bmod 102 = 484 \bmod 102 = 76$

$22^4 \bmod 102 = 76^2 \bmod 102$

$= 5776 \bmod 102 = 64$

$22^8 \bmod 102 = 64^2 \bmod 102$

$= 4096 \bmod 102 = 16$

$22^{16} \bmod 102 = 16^2 \bmod 102 = 52$

$22^{32} \bmod 102 = 52^2 \bmod 102$

$= 2704 \bmod 102 = 52$

$22^{64} \bmod 102 = 52^2 \bmod 102 = 52$

$\vdots$

$22^{256} \bmod 102 = 52$

$\Rightarrow (22^{256} . 22^{64} . 22^4 . 22^2) \bmod 102$

$ab \bmod m = (a \bmod m \,.\, b \bmod m) \bmod m$

$a = 22^{256} . 22^{64} \bmod 102 = (52 . 52) \bmod 102$

$= 52$

$b = 22^4 . 22^2 \bmod 102 = (76 . 64) \bmod 102$

$= 4864 \bmod 102$

$= 70$

$ab \bmod 102 = (70 . 52) \bmod 102 = 70$

$\therefore\ 22^{326} \bmod 102 = 70$

2206028932
ALDEN LUTHFI

c. $\gcd(a,b) = \gcd(b, a \bmod b)$

$\gcd(703, 70)$
$= \gcd(70, 3)$
$= \gcd(3, 1) = 1$

karena kedua angka memiliki faktor terbesar 1
maka keduanya koprima

2. Chinese Remainder Teorem (CRT)

1. $x \bmod 3 = 2$
2. $x \bmod 4 = 3$
3. $x \bmod 5 = 4$
4. $x \bmod 7 = 5$

misal $M = 3 \times 4 \times 5 \times 7 = 420$

misal :

$M_1 = 4 \times 5 \times 7 = 140 \rightarrow 140\, a_1 \equiv 1 \bmod 3 \rightarrow a_1 = 2$
$M_2 = 3 \times 5 \times 7 = 105 \rightarrow 105\, a_2 \equiv 1 \bmod 4 \rightarrow a_2 = 1$
$M_3 = 3 \times 4 \times 7 = 84 \rightarrow 84\, a_3 \equiv 1 \bmod 5 \rightarrow a_3 = 4$
$M_4 = 3 \times 4 \times 5 = 60 \rightarrow 60\, a_4 \equiv 1 \bmod 7 \rightarrow a_4 = 2$

maka dari itu $x = (2 \cdot 140 \cdot 2 + 3 \cdot 105 \cdot 1 + 4 \cdot 84 \cdot 4 + 5 \cdot 60 \cdot 2) \bmod 420$
$= (560 + 315 + 672 + 600) \bmod 420$
$= 299$

3. $a \cdot b = \gcd(a,b) \cdot \operatorname{lcm}(a,b)$

$\therefore \operatorname{lcm}(a,b) = \dfrac{ab}{\gcd(a,b)} = \dfrac{3^5 \cdot 4^3 \cdot 6^8 \cdot 8^{10}}{3^2 \cdot 4 \cdot 6^3} = 3^3 \cdot 4^2 \cdot 6^5 \cdot 8^{10}$

2206028932
ALDEN LUTHFI

4. Proof by induction

Base case :

$P(n): n^2 + 2 \equiv 3 \pmod 8$

$P(1): 1 + 2 \equiv 3 \pmod 8 \rightarrow$ benar

inductive case

asumsikan $P(k)$ bernilai benar untuk ~~semua~~ sembarang k bilangan ganjil

$P(k): k^2 + 2 \equiv 3 \pmod 8$
atau $k^2 + 2 = 8n + 3$ untuk $n \in \mathbb{Z}^+$

maka bilangan ganjil berikutnya adalah $k+2$

$P(k+2): (k+2)^2 + 2 \equiv 3 \pmod 8$
$(k+2)^2 + 2$
$= (k^2 + 4k + 4 + 2)$
$= (k^2 + 2) + (4k + 4)$
$= (8n + 3) + (4(2a+1) + 4) \rightarrow$ definisi bilangan ganjil , $a \in \mathbb{Z}^+$
$= (8n + 3 + 8a + 8)$
$= (8(n + a + 1) + 3) \rightarrow (k+2)^2 + 2 \equiv 3 \pmod 8$

telah terbukti kebenaran $P(k) \rightarrow P(k+2)$ untuk bilangan ganjil maka benar untuk $n > 0$, $n^2 + 2 \equiv 3 \pmod 8$

2206028932
ALDEN LUTHFI

5. Direct proof

$a \mid c$ maka $c = am$ untuk $m \in \mathbb{Z}$
$b \mid d$ maka $d = bn$ untuk $n \in \mathbb{Z}$

$cd = ab(mn)$ sehingga dapat dilihat $\frac{cd}{ab} \in \mathbb{Z}$ karena $m \in \mathbb{Z}$ dan $n \in \mathbb{Z}$ sehingga $ab \mid cd$ ▨

6. $20x^2 + 23x \equiv 17 \pmod{23}$, $x \in \mathbb{Z}$
→ $20x^2 + 23x - 17 \equiv 0 \pmod{23}$

$20x^2 + 23x - 17 = 23m$, $m \in \mathbb{Z}$
→ misal $m = x + 1$
maka $20x^2 - 17 = 23.(1)$
$= 20x^2 + 6 = 23(2)$

→ $20x^2 \equiv 17 \pmod{23}$
misal $x^2 = y$
$20y \equiv 17 \pmod{23}$

Extended euclidean Algorithm : (rekursi)
$\gcd(a,b) = \gcd(b, a \% b)$
dimana $a \% b = a - \lfloor \frac{a}{b} \rfloor b$
maka jika $ax + by = \gcd(a,b)$
$bx' + (a - \lfloor \frac{a}{b} \rfloor b)y' = \gcd(b, a\%b)$ } sama
$= ay' + b(x' - \lfloor \frac{a}{b} \rfloor y')$
maka $x = y'$ dan $y = x' - \lfloor \frac{a}{b} \rfloor y'$
dan jika $b = 0$, $x = 1$ dan $y = 0$ ($\gcd(a,0)$ dianggap $= a$)

		$a(x) + b(y)$
$\gcd(23, 20)$	→	$23(7) + 20(-8) = 1$
$\gcd(20, 3)$	→	$20(-1) + 3(7) = 1$
$\gcd(3, 2)$	→	$3(1) + 2(-1) = 1$
$\gcd(2, 1)$	→	$2(0) + 1(1) = 1$
$\gcd(1, 0)$	→	$1.(1) + 0.(0) = 1$

2206028932
ALDEN LUTHFI

karena $1 = 23(7) - 20(8)$
$-8.20 \equiv 1 \pmod{23}$
$-8 \equiv 15 \pmod{23}$

$15.20y \equiv 17.15 \pmod{23}$
$y \equiv 255 \pmod{23}$
$x^2 \equiv 25 \pmod{23}$

$x \equiv 5 \pmod{23}$ $x \equiv -5 \pmod{23}$
▨ $x \equiv 18 \pmod{23}$ ▨

7. (i) bilangan ganjil + bilangan genap = bilangan ganjil
(ii) bilangan genap + bilangan genap = bilangan genap
(iii) bilangan ganjil + bilangan ganjil = bilangan genap
(iv) bilangan genap tidak akan membagi bilangan ganjil karena semua kelipatan bilangan genap adalah genap
(v) bilangan ganjil . bilangan ganjil = bilangan ganjil

→ jika x ganjil
$x + 5$ → genap ... (iii)
$3x + 52$ → ganjil ... (v) dan (i)
$x + 5 \nmid 3x + 52$ ... (iv) terbukti untuk x ganjil ▨

→ jika x genap dan $x + 5 \mid 3x + 52$
$3x + 52 = (x+5)m$
$3x + 52 = mx + 5m$
$x = \frac{5m - 52}{(3 - m)}$
↳ $m = 4$ memenuhi dengan $x = 32$
sehingga $x + 5 \mid 3x + 52$ → $37 \mid 148$ terbukti benar

2206028932
ALDEN LUTHFI

(8.) tidak karena x dan z masih bisa memiliki faktor yang sama

contoh :

$x = 2 \cdot 3 = 6$
$y = 5 \cdot 7 = 35$
$z = 2 \cdot 9 = 18$

y koprima dengan x dan z namun x tidak koprima dengan z

(9.) Andi harus mengecek angka prima $\leq \lfloor\sqrt{2459}\rfloor = 49$ karena jika 2459 memiliki faktor > 49 hasil baginya adalah bilangan yang < 49 yang pasti memiliki faktor < 49 juga sehingga tidak mungkin ~~sehingga~~ hanya perlu mengecek prima < 49 saja.

(10) (a.) fungsi rekursi Extended Euclidean Algorithm di No 6

$$
\begin{aligned}
& && ax + by \\
\gcd(1074, 79) &\rightarrow & 1074(37) + 79(-503) &= 1 \\
\gcd(79, 47) &\rightarrow & 79(-22) + 47(37) &= 1 \\
\gcd(47, 32) &\rightarrow & 47(15) + 32(-22) &= 1 \\
\gcd(32, 15) &\rightarrow & 32(-7) + 15(15) &= 1 \\
\gcd(15, 2) &\rightarrow & 15(1) + 2(-7) &= 1 \\
\gcd(2, 1) &\rightarrow & 2(0) + 1(1) &= 1 \\
\gcd(1, 0) &\rightarrow & 1(1) + 0(0) &= 1 \\
& && ax' + by'
\end{aligned}
$$

maka $\gcd(79, 1074) = 1 = 79(-503) + 1074(37)$

(b.) karena $79(-503) = 1 + 1074(-37)$
maka $-503 \equiv 571 \pmod{1074}$ adalah invers modulo dari 79 mod 1074