Lisa Maszkiewicz

Problem Set 3 3/9/20

2. Repeated Squaring Method to calculate:
$652^{853} \bmod 4847$

$652^2 = 425104 \bmod 4847 = 3415 \bmod 4847$

(mod 4847) $652^4 \equiv 3415^2 \equiv 343,\ 343^2 \equiv 1321,\ 1321^2 \equiv 121,$

$121^2 \equiv 100,\ 100^2 \equiv 306,\ 306^2 \equiv$ ...

~This is when I realized there was a lot more work to do and typed it up on the computer~

1. First we need to calculate $W^{-1} \pmod{2647}$ $W = 1036$

$2647 = 1036 \times 2 + \underline{575}$

$1036 = 575 \times 1 + \underline{461}$

$575 = 461 \times 1 + \underline{114}$

$461 = 114 \times 4 + \underline{5}$

$114 = 5 \times 22 + \underline{4}$

$5 = 4 \times 1 + \underline{1}$

a	b	$\lfloor a/b \rfloor$	d	x	y
2647	1036	2	1	-209	534
1036	575	1	1	116	-209
575	461	1	1	-93	116
461	114	4	1	23	-93
114	5	22	1	-1	23
5	4	1	1	1	-1
4	1	4	1	0	1
1	0		1	1	0

$W^{-1} = 534$ Next, for each message unit:
$(X_i \cdot W^{-1}) \bmod 2647$, then knapsack (A, answer)

$(2723 \cdot 534) \bmod 2647 = 879$

$(A, 879) = 0010101010 = 170 = (26 \cdot 6) + 14 = $ GO

$(3532 \cdot 534) \bmod 2647 = 1424$ $(A, 1424) = 0001010001 = $ DD

$(6132 \cdot 534) \bmod M = 149$ $(A, 149) = 0101110000 = 368 = $ OE

$(5713 \cdot 534) \bmod M = 1398$ $(A, 1398) = 0111100001 = 481 = $ SN

$(10008 \cdot 534) \bmod M = 2626$ $(A, 2626) = 0101111111 = 383 = $ OT

$(4682 \cdot 534)$ " $= 1420$ $(A, 1420) = 0110010001 = 401 = $ PL

$(2816 \cdot 534)$ " $= 248$ $(A, 248) = 0000011000 = 24 = $ AY (cont.) 1. $(5762 \cdot 534) \bmod M = 1094$ $(A, 1094) = 0001010110 = DI$

$(2940 \cdot$ " $) \bmod M = 289$ $(A, 298) = 0000111000 = CE$

answer = GOD DOES NOT PLAY DICE!

3. We want to prove $d' \leq d$ where
$d = \gcd(a,b)$ and $d' = \gcd(b, a \bmod b)$
So if $d' = \gcd(b, a \bmod b)$, then $d' | b$ and $d' | a \bmod b$
$a \bmod b = a - \lfloor a/b \rfloor b \Rightarrow a = a \bmod b + \lfloor a/b \rfloor b$
$\Rightarrow a$ is a linear combination of b and $a \bmod b$.
$\therefore$ by 1.4 (iii) $d' | a$. So if $d' | a$ and $d' | b$,
d' is a common denominator of a and b.
But since $d = \gcd(a,b)$, $d' \leq d$. ■
To complete the full proof, we've now shown
$d \leq d'$ and $d' \leq d$, $\Rightarrow d = d'$ for any $a \geq 0, b \geq 0$
$\therefore \gcd(a,b) = \gcd(b, a \bmod b)$

4. Complete proof of Thm 1.13:
$\exists x, y$ s.t. $ax + by = 1$, then $\gcd(a,b) = 1$
$\Rightarrow$ Assume $ax + by = 1$, ~~then 1 is a linear combination of a and b. Therefore by 1.4(iii) gcd(a,b)|1 d|1 and b|1. Because 1 is the smallest positive integer,~~
and there is some $d = \gcd(a,b)$. So $d | a$ and $d | b$. $\Rightarrow d | ax + by \Rightarrow d | 1$. Because 1 is the smallest positive integer $d = 1$.
$\therefore$ If $ax + by = 1$, $\gcd(a,b) = 1$ ■

Lisa Maszkiewicz

3/18/20

5. Prove: If $a|b$, $b|c$ and $\gcd(a,b)=1$ then $ab|c$

Assume $a|b$, $b|c$, $\gcd(a,b)=1$. ~~By 1.4(i) $a|c$~~

In my math classes w/ problems like these I learned to multiply/substitute until you get the term you need. :)

If $\gcd(a,b)=1$ then from problem 4) we know for some $x,y \in \mathbb{Z}$ $ax+by=1$

Also we know for some ~~am~~ $m,n \in \mathbb{Z}$, $\underbrace{am=c \;\&\; bn=c}$

Let's $c*(ax+by=1) \Rightarrow \{cax+byc=c\} \leftarrow$ substitute

$a x \underset{bn}{c} + b y \underset{am}{c} = c \Rightarrow axbn+byam=c$

$\Rightarrow \dfrac{(ab)xn+(ab)ym=c}{ab}$

Because $x,n,y,m \in \mathbb{Z}$, $xn+ym \in \mathbb{Z}$ so therefore $c/(ab) \in \mathbb{Z}$ and therefore $ab|c$. ■

6. Prove: If $m \perp n$, $a \equiv b \pmod m$ and $a \equiv b \pmod n$, then $a \equiv b \pmod{mn}$

Proof: By Thm 3.2 pt (i), if $a \equiv b \pmod m$ and $a \equiv b \pmod n$, then $m|a-b$ and $n|a-b$, respectively.

Then, by the theorem we proved in problem 5: (If $a|c$, $b|c$, and $\gcd(a,b)=1$ (then $ab|c$)) and since we know if $m \perp n$ ~~are~~ then $\gcd(m,n)=1$.

We have $m|a-b$, $n|a-b$, and $\gcd(m,n)=1$

$\therefore$ $mn|a-b$. We then use 3.2(i) again and get $a \equiv b \pmod{mn}$ ■

7. Let $a \in \mathbb{Z} \geq 0$, let $b, c, M \in \mathbb{Z} > 0$, let $d = \gcd(c, M)$

Prove: If $\exists\, k$ s.t. $a + kc \equiv b \bmod M$, then $d \mid (b-a)$

Proof: We want to show $d \mid (b-a)$ or $\gcd(c, M) \mid (b-a)$.

$a + kc \equiv b \bmod M \Rightarrow a + kc = b + Mx$, $x \in \mathbb{Z}$

$\Rightarrow b - a = kc - Mx$

We know by def of gcd that $\gcd(c, M) \mid c$ and $\gcd(c, M) \mid M$ and by Prop 1.4 (iii)

$\rightarrow \gcd(c, M) \mid yc + zM$ for ~~some~~ any $y, z \in \mathbb{Z}$.

We can just say $y = k$ and $z = -x$

and we have $b - a = yc + zM$

and since $\gcd(c, M) \mid yc + zM = b - a$

$\Rightarrow \gcd(c, M) \mid (b-a)$ ■.