Discrete Maths Supervision 3

dlorgan Schulde

3.1.1 $CD(666, 330) = CD(2 \cdot 3^2 \cdot 37, 2 \cdot 3 \cdot 5 \cdot 11)$

$= \{2^0 3^0, 2^0 3^1, 2^1 3^0, 2^1 3^1\}$

$= \{1, 2, 3, 6\}$

2. $\gcd(212121\,21, 12121212) = \gcd(12121212, 9090909)$

$= \gcd(9090909, 8030303)$

~~$= \gcd(8030303, 6060606)$~~

~~$= \gcd$~~

$= 8030303$

3. $\gcd(m,n) \mid m \Rightarrow \gcd(m,n) \mid km \quad \forall k \in \mathbb{Z}$

$\gcd(m,n) \mid n \Rightarrow \gcd(m,n) \mid ln \quad \forall l \in \mathbb{Z}$

$\therefore km = a \gcd(m,n)$ for some integer a

$ln = b \gcd(m,n)$ for some integer b

$\therefore km + ln = (a+b) \gcd(m,n)$

$\therefore \gcd(m,n) \mid (km + ln)$

4. $\gcd(30,22) = \gcd(22,8) = \gcd(8,6) = \gcd(6,2) = 2$

$2 = 3 \cdot 30 + (-4) \cdot 22$

$\therefore x = 3, \; y = -4$

$2 = (-8) \cdot 30 + 11 \cdot 22$

$\therefore x' = -8, \; y' = 11$

5. RTP: $\forall m,n \in \mathbb{Z}^+$, $(\exists k,l \in \mathbb{Z}$ s.t. $km+ln=1 \iff \gcd(m,n)=1)$

By universal instantiation, let m, n arbitrary integers > 0

Proof of "$\Rightarrow$"
Assume $\exists k,l \in \mathbb{Z}$ s.t. $km+ln=1$
Instantiating, let k,l s.t. $km+ln=1$
RTP: $\gcd(m,n)=1$
By question 3, $\gcd(m,n) \mid (km+ln)$
Equivalently, $\gcd(m,n) \mid 1$
$\gcd(m,n) > 0$
$\therefore \gcd(m,n)=1$ ∎

Proof of "$\Leftarrow$"
Assume $\gcd(m,n)=1$
RTP: $\exists k,l \in \mathbb{Z}$ s.t. $km+ln=1$
~~By question 3, $\gcd(m,n) \mid (am+bn)$ for all arbitrary $a,b \in \mathbb{Z}$~~
~~Equivalently, $1 \mid$~~
By Euclid's algorithm, $\gcd(m,n) =$
$\gcd(n+am, m)$ for arbitrary $a \in \mathbb{Z}$
$= \gcd(b(am+n)+m, am+n)$ for arbitrary $b \in \mathbb{Z}$
$= \gcd(k'm+l'n, am+n)$ for some $k', l' \in \mathbb{Z}$
$= 1$
Let $k' = an$ for some $a \in \mathbb{Z}$
Let $l' = \frac{1-k'm}{n}$
$\therefore k'm+l'n = 1$
RTP: $l' \in \mathbb{Z}$
Equivalently, $n \mid 1-k'm$
Equivalently, $n \mid 1-nm$
Equivalently, true
By theorem 7 c), $\exists k', l'$ s.t. $\gcd(m,n) = k'm+l'n = 1$ ∎

6. RTP $\forall u \in \mathbb{Z}\ \forall p \in \mathbb{P}\ \ u^2 \equiv 1 \pmod p \Rightarrow u \equiv 1 \pmod p \vee u \equiv -1 \pmod p$

Let u, p arbitary.

Assume $u^2 \equiv 1 \pmod p$
RTP: $u \equiv 1 \pmod p \vee u \equiv -1 \pmod p$

$u^2 - 1 \equiv 0 \bmod p$
$\therefore u^2 - 1 \mid p$
$\therefore (u-1)(u+1) \mid p$
$\therefore (u-1) \mid p \vee (u+1) \mid p$
$\therefore u - 1 \equiv 0 \pmod p \vee u + 1 \equiv 0 \pmod p$
$\therefore u \equiv 1 \pmod p \vee u \equiv -1 \pmod p$

■

First prove "$\Leftarrow$"

3.2.1. $\forall d \in \mathbb{Z},\ (d \mid m \wedge d \mid n) \Rightarrow d \mid \gcd(m,n)$

Take $d = m$.
$m \mid m \wedge m \mid n \Rightarrow m \mid \gcd(m,n)$
Equivalently, $m \mid n \Rightarrow m \mid \gcd(m,n)$
Since $\gcd(m,n) \mid m$,
$m \mid n \Rightarrow \gcd(m,n) = m$

Now prove "$\Rightarrow$"
$\gcd(m,n) \mid n$
$\therefore \gcd(m,n) = m \Rightarrow m \mid n$

■

2. Assume $\gcd(a,c) = 1$
RTP: $\gcd(ab, c) = \gcd(b, c)$
By distributivity,
$\gcd(ab, bc) = b \gcd(a,c) = b$
By associativity,
$\gcd(\gcd(ab, bc), c) = \gcd(b,c) = \gcd(ab, \gcd(bc, c)) = \gcd(ab, c)$

■

3. First prove "⇒"

Assume $ni \equiv nj \pmod{m}$

Equivalently $n(i-j) \mid m$

RTP: $i \equiv j \pmod{\frac{m}{\gcd(m,n)}}$

Equivalently $i-j \mid \frac{m}{\gcd(m,n)}$

~~Case 0: $n \mid m$~~

~~$\gcd(m,n) = n$~~

~~$\therefore \frac{m}{\gcd(m,n)} = \frac{m}{n}$~~

$n(i-j) \mid m$

$\therefore \frac{n}{\gcd(m,n)}(i-j) \mid \frac{m}{\gcd(m,n)}$

$\gcd\left(\frac{n}{\gcd(m,n)}, \frac{m}{\gcd(m,n)}\right) = \frac{1}{\gcd(m,n)} \gcd\left(\frac{n\gcd(m,n)}{\gcd(m,n)}, \frac{m(\gcd(m,n))}{\gcd(m,n)}\right)$

$= \frac{1}{\gcd(m,n)} \cdot \gcd(m,n)$

$= 1$

$\therefore i-j \mid \frac{m}{\gcd(m,n)}$

Next prove "⇐"

Assume $i \equiv j \pmod{\frac{m}{\gcd(m,n)}}$

Equivalently $i-j \mid \frac{m}{\gcd(m,n)}$

$i-j \mid m$

$\therefore i \equiv j \pmod{(m)}$

$\therefore ni \equiv nj \pmod{(m)}$

□

5. $\gcd(m,n) = \gcd(p,q) = 1$

$\therefore am+bn = cp+dq = 1$ for some $a, b, c, d \in \mathbb{Z}$

Assume $qm = pn$

~~$aqm + bqn = cpq + dq^2 = q$~~

~~$\therefore n(p+bq) =$~~

~~$\therefore \left(\frac{ap}{q} + b\right)n =$~~

~~$\therefore (am+bn)(cp+dq) = 1$~~

~~$acpm + bcpn + adqm + bdqn = 1$~~

$\therefore \gcd(pm, pn) = p$

$\therefore \gcd(pm, qm) = p$

~~$\gcd(p,q) = pm$~~

$\therefore m \gcd(p,q) = p$

$\therefore m = p$

$\therefore n = q$ ∎

6. $\gcd(13a+8b, 5a+3b) = \gcd(5a+3b, 3a+2b)$
$= \gcd(3a+2b, 2a+b)$
$= \gcd(2a+b, a+b)$
$= \gcd(a+b, a)$
$= \gcd(a, b)$

∎

7a.

$\bar{n}$	$\bar{n}^2$
1	1
2	1

$\pmod 3$

b

$\bar{n}$	$\bar{n}^2$
1	1
3	1
5	1
7	1

$\pmod 8$

c. p is a prime $>3 \Rightarrow p$ is not divisible by 3 $\wedge$ p is odd

$\Rightarrow p^2 \equiv 1 \pmod 3 \wedge p^2 \equiv 1 \pmod 8$

$\Rightarrow p^2 \equiv 1 \pmod{24}$

$\Rightarrow p^2 - 1 \mid 24$

8.

$\bar{n}$	$\bar{n}^2$	$\bar{n}^4$	$\bar{n}^8$	$\bar{n}^{12}$	$\bar{n}^{13}$
0	0	0	0	0	0
1	1	1	1	1	1
2	4	6	6	6	2
3	9	1	1	1	3
4	6	6	6	6	4
5	5	5	5	5	5
6	6	6	6	6	6
7	9	1	1	1	7
8	4	6	6	6	8
9	1	1	1	1	9

$\pmod{10}$

$\therefore n \equiv n^{13} \pmod{10}$

9. Assume $\gcd(l, m \cdot n) = 1$

$\therefore \exists a, b \in \mathbb{Z}$ such that

$al + bmn = 1$

$\therefore al + (bn)n = 1 \wedge a(l + (bn)m = 1$

$\therefore \exists a, b', c' \in \mathbb{Z}$ such that $al + b'n = 1 \wedge al + c'm = 1$

$\therefore \gcd(l, m) = 1 \wedge \gcd(l, n) = 1$

10a. $77x \equiv 1 \pmod{40}$

$\therefore 7x \equiv 1 \pmod{40}$

$\therefore x \equiv 23 \pmod{40}$

b. $12y \equiv 30 \pmod{54}$

~~$12y \equiv 6 \pmod{54}$~~

$\therefore y \equiv 16 \pmod{54}$

c. $3z \equiv 18 \pmod{21}$

$3z \equiv 2 \pmod{17}$

$\therefore 3z \equiv 1580 + 546 \mod (357)$

$\equiv 291 \mod (357)$

11 i. $2^{-1} \equiv 4 \pmod{7}$

ii $7^{-1} \equiv 23 \pmod{40}$

iii. $13^{-1} \equiv 16 \pmod{23}$

12 $22^{12001} = 2^{12001} \cdot 11^{12001}$

$175 = 5^2 \cdot 7$

$\therefore \gcd(22^{12001}, 175) = 1$

$\therefore 22^{12001}$ has a multiplicative inverse mod 175

$\therefore [22^{12001}]_{175}$ has a multiplicative inverse mod 175