Problem Set 9: Discrete Mathematics Name Theepakorn Phayonrat ID 67011352

1. For m = 6 and n = 15, list some positive linear combinations mx + ny for integers x, y. What is the smallest positive linear combination you can get? What is gcd(m, n)?

$x = 1, y = 1$ give $mx + ny = 21$;

$x = -2, y = 1$ gives $mx + ny = 3$;

You can't get linear combination that smaller than 3 and $\gcd(6, 15) = 3$

2. Show that if d|mn, then d|gcd(m,d).n.

Suppose $d | mn$. By Bezout, there're $x, y$ for which $\gcd(m, d) = mx + dy$.

Multiply both side by n to get $\gcd(m, d) \cdot n = xmn + ynd$; $n \in \mathbb{Z}$

d divide the second term on RHS (it is a multiple of d). d also divides the first term on the RHS because

$d | mn$, so $mn = \alpha d$; $\alpha \in \mathbb{Z}$

$\therefore$ the RHS is $(x\alpha + yn)d$, that is d divides the sum on the RHS.

$\therefore$ d must divide the LHS which was to be shown

3. Let d,d' be relatively prime. Show that if d|n and d'|n, then dd'|n.

We're given that $\gcd(d, d') = 1 = dx + d'y$ (Bezout identity).

Multiply both sides by n to get $n = xdn + yd'n$; $n \in \mathbb{Z}$

Since $d | n$, $n = \alpha d$; $\alpha \in \mathbb{Z}$.

Since $d' | n$, $n = \alpha' d'$; $\alpha' \in \mathbb{Z}$

Rewriting the equation above, $n = x\alpha' d d' + y\alpha d d' = (x\alpha' + y\alpha) dd'$, which means $dd' | n$ as was to be shown.

4. Show that gcd(gcd(ℓ, m), n) = gcd(ℓ, gcd(m, n)).

Let $D = \gcd(\gcd(\ell,m),n)$ and $D' = \gcd(\ell,\gcd(m,n))$. We have to show $D \leq D'$ and $D' \leq D$

5. Compute the remainder when $5^{2015}$ is divided by: (i) 3 and (ii) 11

$5^2 \bmod 3 \equiv 1$

$(5^2)^{1007} \bmod 3 \equiv 1^{1007} \bmod 3$

$5\left[(5^2)^{1007}\right] \bmod 3 \equiv 5(1^{1007}) \bmod 3$

$\equiv 5 \bmod 3$

$5^{2015} \bmod 3 \equiv 2$

$5^5 \bmod 11 \equiv 1$

$(5^5)^{403} \bmod 11 \equiv 1^{403} \bmod 11$

$5^{2015} \bmod 11 \equiv 1$

6. Show that 15 does not have a multiplicative inverse for modulus 6.

With contradiction, assume 15 has a multiplicative inverse k

Theepakorn Phayonrat 67011352

1. Use the Euclidean algorithm to Express gcd (30, 78) as linear combination of 30 and 78.

| | | |
|---|---|---|
| gcd(30, 78) | = gcd(18, 30) | 18 = 78 − 2(30) |
| | = gcd(12, 18) | 12 = 30 − 1(18) |
| | = gcd(6, 12) | 6 = 18 − 1(12) |
| | = gcd(0, 6) | 0 = 12 − 3(6) |
| | = 6 # | |

2. Which integers in {1, 2, ..., 8} have multipliactive inverse modulo of 9?

We need to show that which numbers has gcd with 9 and equal to 1: They are 1, 2, 4, 5, 7, 8 #