Midterm 1 / October 20, 2010 / MAT 3233.001 / Modern Algebra

Note Title 10/21/2010

1. Use induction to show that for $n \geq 1$ the partial sum

$$1 + 7 + 13 + \ldots + (6n - 5) = \sum_{k=1}^{n} (6k - 5)$$

can be expressed in closed form by $3n^2 - 2n$.

Basis: $n = 1$ $\quad 1 = 3 \cdot 1^2 - 2 \cdot 1 = 1$ ☺

Assume $1 + \ldots (6(n-1) - 5) = 3(n-1)^2 - 2(n-1)$

Then $1 + \ldots + (6n-5) = 1 + \ldots (6(n-1) - 5) + (6n - 5)$

$= 3(n-1)^2 - 2(n-1) + 6n - 5$

$= 3n^2 - 6n + 3 - 2n + 2 + 6n - 5 = 3n^2 - 2n$ ☺

Check: $\sum_{k=1}^{n} (6k - 5) = 6 \sum_{k=1}^{n} k - 5 \sum_{k=1}^{n} 1 = 6 \frac{n(n+1)}{2} - 5n$

$= 3n^2 + 3n - 5n = 3n^2 - 2n$ ☺

2. Use Euclid's algorithm to find $(75, 27)$ and $s, t \in \mathbf{Z}$ such that $(75, 27) = 75s + 27t$.

$75 = 2 \cdot 27 + 21$

$27 = 21 + 6$

$21 = 3 \cdot 6 + 3$

$6 = 2 \cdot 3$

$\therefore \boxed{(75, 27) = 3}$

Solve for remainders →

$21 = 75 - 2 \cdot 27$

$6 = 27 - 21$

$3 = 21 - 3 \cdot 6$

$= 21 - 3(27 - 21)$

$= -3 \cdot 27 + 4 \cdot 21$

$= -3 \cdot 27 + 4(75 - 2 \cdot 27)$

$= -11 \cdot 27 + 4 \cdot 75$

$\therefore \boxed{s = 4, \; t = -11}$

3. Find all solutions of the linear congruences

(a) $3x \equiv 5 \bmod 13$ (b) $5x \equiv 15 \bmod 20$

a) Euclid: $13 = 4 \cdot 3 + 1$, so $1 = 13 - 4 \cdot 3$

so $-4 \cdot 3 \equiv 1 \bmod 13$

Multiply Both sides by -4: $x = -4 \cdot 5 = -20 \equiv 6 \bmod 13$

b) Divide by 5: $x \equiv 3 \bmod 4$ i.e. $x \equiv 3, 7, 11, 15, 19 \bmod 20$

4. Compute 3^{42} modulo 7 by repeated squaring and reduction. Show work.

$42 = 32 + 8 + 2 = [101010]_2$

xSSxSSxS : $3, 2, 4, 5, 4, 2, 6, 1$ $\therefore$ $3^{42} \equiv 1 \bmod 7$

Check: By Fermat $3^6 \equiv 1 \bmod 7$, so $3^{42} = (3^6)^7 \equiv 1^7 = 1 \bmod 7$

5. Suppose R is a commutative ring (with unity) and let U be the set of all units in R.

(a) Prove that U is a multiplicative group.

(b) Prove that U cannot contain zero divisors.

(c) Describe U for the rings $\mathbf{Z}$, $\mathbf{Z}_m$, and $\mathbf{C}$.

a) Associativity of multiplication is inherited from R

Identity: Since $1 \cdot 1 = 1$, $1 \in U$.

Closure under multiplication: If $a, b \in U$, $\exists a', b'$ $aa' = bb' = 1$,

so $abb'a' = a \cdot 1 a' = aa' = 1$, so $ab \in U$.

Closure under inverses: If $a \in U$, $aa^{-1} = a^{-1}a = 1$, so $a^{-1} \in U$.

b) Suppose $a \in U$, $b \in R$ $ab = 0$. Then $a^{-1}ab = b = 0$ ☺

c) If $R = \mathbb{Z}$, $U = \{1, -1\}$

If $R = \mathbb{Z}_m$, $U = \{k \in \mathbb{Z}_m : (k, m) = 1\}$

If $R = \mathbb{C}$, $U = \mathbb{C} \setminus \{0\}$