

Math 356 — Midterm I — Fall 2007

1

Prove by induction that $1^3 + 2^3 + \dots + n^3 = n^2(n+1)^2/4$ for all $n \geq 1$

Solution 1 For $n = 1$ we verify $1^2(1+1)^2/4 = 4/4 = 1 = 1^3$. By induction

$$\begin{aligned} LHS &= [1^3 + 2^3 + \dots + (n-1)^3] + n^3 = [(n-1)^2(n)^2/4] + n^3 \\ &= (n^2/4)[(n-1)^2 + 4n] = (n^2/4)[n^2 + 2n + 1] = n^2(n+1)^2/4 \end{aligned}$$

2

Find integers x, y such that $868x + 527y = \gcd(868, 527)$.

Solution 2 We determine the gcd as follows:

a	b	$a - b$	$2b - a$	$2a - 3b$	$5b - 3a$	$17a - 28b$
868	527	341	186	165	31	0

So the gcd is 31 and we have $868(-3) + 527(5) = 31$.

3

Suppose a and m are coprime. If $\{x_1, \dots, x_k\}$ is a reduced residue system (RRS) mod m , prove that $\{ax_1, \dots, ax_k\}$ is also an RRS.

State and prove Euler's theorem.

Solution 3 The set $\{ax_1, \dots, ax_k\}$ has $k = \phi(m)$ elements. Since a and x_i are coprime to m , so is ax_i . It remains to prove that the ax_i are incongruent, but since $\gcd(a, m) = 1$, $ax_i \equiv ax_j \pmod{m} \Rightarrow x_i \equiv x_j \pmod{m} \Rightarrow i = j$.

Euler's Theorem: If $\gcd(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$

Proof: By (1) $(ax_1) \dots (ax_k) \equiv x_1 \dots x_k \pmod{m}$. Since $\gcd(m, x_i) = 1$, we can cancel the x_i to get $a^k = a^{\phi(m)} \equiv 1 \pmod{m}$.

4

State the Chinese remainder theorem (CRT). Use the CRT to find an integer x such that $x \equiv 2 \pmod{7}$, $x \equiv 3 \pmod{5}$, and $x \equiv 1 \pmod{3}$. (Show your steps. No credit for guessing an answer.)

Solution 4 CRT: If m_1, \dots, m_k are pairwise coprime, then for any c_1, \dots, c_k the congruences $\{x \equiv c_1 \pmod{m_1}, \dots, x \equiv c_k \pmod{m_k}\}$ have a simultaneous solution x_k . Moreover the general solution is $\{x_k + t(m_1 \dots m_k) : t \in \mathbb{Z}\}$.

We solve the congruences as follows: the first gives $\mathbf{x} = \mathbf{7u} + \mathbf{2}$.

Next $7u + 2 \equiv 3 \pmod{5} \Rightarrow u \equiv 3 \pmod{5} \Rightarrow u = 5v + 3 \Rightarrow \mathbf{x} = \mathbf{35v} + \mathbf{23}$.

Finally $35v + 23 \equiv 1 \pmod{3} \Rightarrow v \equiv 1 \pmod{3} \Rightarrow v = 3t + 1 \Rightarrow \mathbf{x} = \mathbf{105t} + \mathbf{58}$.

5

State the Moebius inversion formula (explaining any symbols you use). Prove that the functions ϕ and e_1 form a Moebius pair.

Solution 5 Moebius inversion formula: $e_0 * \mu = \delta$ where $e_0(n) = 1$ for all n

$$\delta(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}, \mu(n) = \begin{cases} (-1)^r & \text{if } n = p_1 \dots p_r \text{ distinct primes} \\ 0 & \text{otherwise} \end{cases}$$

and $f * g(n) = \sum_{d|n} f(d)g(n/d)$.

We need to show $(\phi * e_0)(n) = e_1(n)$ for all n . Since both sides are multiplicative, it is enough to consider prime powers p^a . In this case we have

$$(\phi * e_0)(p^a) = \sum_{0 \leq b \leq a} \phi(p^b) = (p^a - p^{a-1}) + \dots + (p - 1) + 1 = p^a = e_1(p^a)$$