Discrete Mathematics

COMS 3203 – Fall 2017

http://www.cs.columbia.edu/~amoretti/3203

Practice Exam # 2

Problem 1

1. Recall:

$$\sum_{k=0}^{n} \binom{n}{k} p^k q^{n-k} = (p+q)^n \tag{1}$$

$$\sum_{k=0}^{n} \binom{n}{k} p^k (1-p)^{n-k} = (p+(1-p))^n = 1 \tag{2}$$

$$\tag{3}$$

2. Use the Geometric series:

$$\sum_{k=0}^{\infty} p(1-p)^k = p\sum_{k=0}^{\infty}(1-p)^k = p\Big(\frac{1}{1-(1-p)}\Big) = \frac{p}{p} = 1 \tag{4}$$

3. Expand:

$$\binom{k+r-1}{k} = \frac{(k+r-1)!}{k!(k+r-1-k)!} \tag{5}$$

$$= \frac{(k+r-1)(k+r-2)\cdots(r)\cdots 1}{k!(\cancel{k}+r-1-\cancel{k})!} \tag{6}$$

$$= \frac{(k+r-1)(k+r-2)\cdots(r)\cancel{\cdots 1}}{k!\cancel{(r-1)!}} \tag{7}$$

$$= \frac{(k+r-1)(k+r-2)\cdots(r)}{k!} \tag{8}$$

$$= (-1)^k\frac{(-r)(-r-1)\cdots(-r-k+1)}{k!} = (-1)^k\binom{-r}{k} \tag{9}$$

Therefore:

$$(1-p)^{-r} = \sum_{k=0}^{\infty}\binom{-r}{k}(-p)^k = \sum_{k=0}^{\infty}\binom{k+r-1}{k}p^k \tag{10}$$

$$\sum_{k=0}^{\infty}\binom{k+r-1}{k}(1-p)^r p^k = (1-p)^r(1-p)^{-r} = 1 \tag{11}$$

Problem 2

1. Prove that if $a' \equiv a \bmod n$ and $b' \equiv b \bmod n$ then $(a' \bmod n) \cdot (b' \bmod n) \equiv (a \cdot b) \bmod n$.

   Proof. By Euclid $\exists$ integers q_a, q_b, r_a, r_b such that $a = q_a n + r_a$ and $b = q_b n + r_b$. Plugging into the RHS:

   $$(q_a n + r_a)(q_b n + r_b)\text{mod } n = (q_a q_b n^2 + q_a r_b n + r_a q_b n + r_a r_b)\text{mod } n \tag{12}$$

   All of these terms are divisible by n except for the remainder $r_a r_b$, and therefore ab mod n = $r_a r_b$ mod n. Inspecting the LHS of the congruence confirms that this is what we need to show. □

Problem 3

1. Consider the set $\mathbb{R}^*$ defined as $\mathbb{R} - \{0\}$. Is $(\mathbb{R}^*, +)$ a group? What about $(\mathbb{R}, \times)$?

   $(\mathbb{R}^*, +)$ has no additive identity $e = 0$ such that $a + e = a \; \forall a \in \mathbb{R}^*$. $(\mathbb{R}, \times)$ has no multiplicative inverse for 0 so that $a \times a^{-1} = e$. To see this, note that the multiplicative identity $e = 1$ satisfies $a \times e = a$ $\forall a \in \mathbb{R}$, but that $0 \times b = 0 \neq e \; \forall b \in \mathbb{R}$. Therefore $\forall a \in \mathbb{R} \; \nexists a^{-1}$ s.t. $a \times a^{-1} = e$.

2. Let $\mathcal{S} = \mathbb{R} - \{-1\}$ and define the operation $a * b = a + b + a \times b$. Is $(\mathcal{S}, *)$ a group? Prove or provide a counter example.

   Proof. We need to check the four axioms below:

   (a) $\forall a, b \in \mathcal{S}$, $a * b \in \mathcal{S}$

   (b) $\forall a, b, c \in \mathcal{S}$, $a * (b * c) = (a * b) * c$

   (c) $\exists e \in \mathcal{S}$ s.t. $e * a = a = a * e \; \forall a \in \mathcal{S}$

   (d) $\forall a \in \mathcal{S}$, $\exists a^{-1} \in \mathcal{S}$ s.t. $a^{-1} * a = e = a * a^{-1}$.

   Closure is trivial, as is the associative property.

   $$a * (b + c + bc) = a + b + c + bc + ab + ac + abc \tag{13}$$
   $$(a + b + ab) * c = a + b + ab + c + ac + bc + abc \tag{14}$$

   The identity element $a * e = a$ is $e = 0$ which is verified by applying the definition of the operation:

   $$a + e + ae = a \Longrightarrow e + ae = 0 \Longrightarrow e(1 + a) = 0 \Longrightarrow e = 0 \tag{15}$$

   Similarly we can derive the inverse as follows:

   $$a * b = 0 \Longrightarrow a + b + ab = 0 \Longrightarrow b + ab = -a \Longrightarrow b(1 + a) = -a \Longrightarrow b = \frac{-a}{1 + a} \tag{16}$$

   This is well defined on $\mathcal{S} = \mathbb{R} - \{-1\}$. □

Problem 4

Consider $\mathbb{Z}_p$ and the function $f_a : \mathbb{Z}_p \to \mathbb{Z}_p$ defined $f_a(x) = ax$. Write the functional digraph when $a = 3$ and $p = 11$. What do you notice about the cycle lengths? What happens when $a = 4$ and $p = 17$?

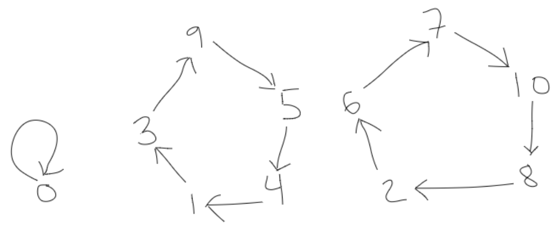

Figure 1: Functional Digraph for $f_3 : \mathbb{Z}_{11} \to \mathbb{Z}_{11}$

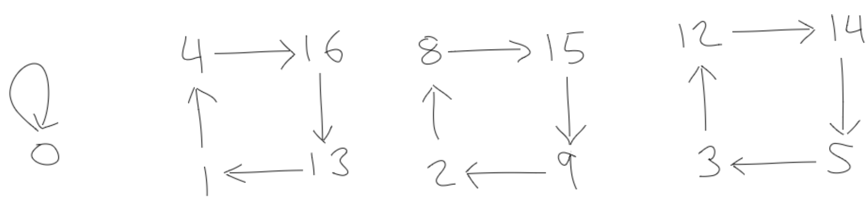

Figure 2: Functional Digraph for $f_4 : \mathbb{Z}_{17} \to \mathbb{Z}_{17}$

Notice that all cycles have the same length excluding zero. When p is prime and $a \not\equiv 0 \bmod p$, there is a positive integer k such that for all $x \in \mathbb{Z}_p$ where $x \neq 0$, the set $S_x = \{x, xa, xa^2, \cdots\}$ has *exactly* k elements.

Problem 5

1. $a^{p-1} \equiv 1(\mod p)$, multiply by a to verify the second formula is correct. Any Carmichael number will satisfy Fermat's Little Theorem. For example, try $561 = 3 \times 11 \times 17$.

2. Take $x \equiv 2 \bmod 4$ and $x \equiv 1 \bmod 2$ which has no solution, and $x \equiv 2 \bmod 4$ and $x \equiv 2 \bmod 6$ for two solutions mod 24 which are 2 and 14.

Problem 6

Euler's Totient function $\phi(m)$ counts the numbers up to m relatively prime to m. Prove for any prime p:

$$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k\Big(1 - \frac{1}{p}\Big) \tag{17}$$

Proof. First note that if p is prime, then $1, 2, \cdots, p-1$ are all relatively prime to p. Therefore $\phi(p) = p - 1$. We now need to consider powers of primes. An integer $x \in \mathbb{Z}$ is relatively prime to p^k if and only if it is not divisible by p. That is, $gcd(x, p^k) = 1$ iff $p \nmid x$. Within the interval $[0, p^k - 1]$ there are p^{k-1} integers not relatively prime to p. That is, np integers where $n = 0, 1, 2, , \cdots p^{k-1} - 1$ not relatively prime to p with $p^k - p^{k-1}$ integers relatively prime to p. Therefore $\phi(p^k) = p^k - p^{k-1}$. Factor out p^k to complete the proof. $\square$

Problem 7

By the fundamental theorem of arithmetic, n can be factorized into m prime numbers.

$$n = \prod_{i=1}^{m} p_i^{k_i} = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m} \tag{18}$$

Use this to show that for $n \in \mathbb{Z}$ where $n > 1$:

$$\phi(n) = n\Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big) \cdots \Big(1 - \frac{1}{p_m}\Big) \tag{19}$$

Proof. We can use the result given in class that the Totient of the product of two relatively prime numbers is the product of their Totient. That is, when $m = m_1 m_2$ and $gcd(m_1, m_2) = 1$:

$$\phi(m) = \phi(m_1)\phi(m_2) \tag{20}$$

Repeatedly applying this result:

$$\phi(m_1 \cdots m_r) = \phi(m_1)\phi(m_2) \cdots \phi(m_r) \tag{21}$$

We know that $\phi(p^k) = p^k(1 - \frac{1}{p})$ and so we can conclude $\phi(n) = n \prod_{p \nmid n}(1 - \frac{1}{p})$ $\square$