MATH6222: Homework #8

2017-04-29

Instructor: Dr. David Smyth

Tutor: Mark Bugden (Wednesday 1-2pm)

Rui Qiu u6139152

Problem 1

Variations on Wilson's Theorem
(a) Prove that if p is prime, $2(p-3)!+1$ is divisible by p.

Proof: First we claim that $p \geq 3$, otherwise, $p-3<0$. Recall Wilson's Theorem which states

$$(p-1)! \equiv -1 \mod p$$

.
We also know that $(p-1)! = (p-1) \cdot (p-2) \cdot (p-3)!$. Since we've already claim that $p \geq 3$, then $(p-1) \cdot (p-2) \equiv (-1) \cdot (-2) \equiv 2 \mod p$.

Therefore, $(p-1)! \equiv 2(p-3)! \equiv -1 \mod p$. In other words, $2(p-3)!+ \equiv 0 \mod p$, $2(p-3)!+1$ is divisible by p.

■

(b) Prove that if p divides $(p-1)!+1$, then p is prime. (This is the converse to Wilson's Theorem.)

Proof: We try to prove the contrapositive of this statement: *If p is not prime, then p does not divide* $(p-1)!+1$.

Since p is not a prime now, suppose $p = m \cdot t$ where m, t are two positive integers smaller than p. Obviously, m, t included in the factorial $(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-2) \cdot (p-1)$. Therefore,

$$\begin{aligned}
(p-1)! &\equiv 0 \mod (m \cdot t) \\
(p-1)! &\equiv 0 \mod p \\
(p-1)! &\not\equiv -1 \mod p
\end{aligned}$$

So we proved the contrapositive of our desired statement. We are done.

■

Problem 2

An important equivalence relation in analysis. Fix a function $f : \mathbb{R} \to \mathbb{R}$, and let $O(f)$ denote the set of functions $g : \mathbb{R} \to \mathbb{R}$ for which there exists positive constants c and a such that $|g(x)| \leq c|f(x)|$ for all $x > a$. Now let S denote the set of all functions from $\mathbb{R}$ to $\mathbb{R}$, and define a relation R on S by setting $(g, h) \in R$ if and only if $g - h \in O(f)$. Prove that R

Problem 2 continued on next page. . .

is an equivalence relation.

Proof:

- **Reflexive property:** Let c, a be arbitrary positive constants, we always have $|g(x) - g(x)| = 0 \leq c|f(x)|, \forall x > a$. In fact, this holds for any $x \in \mathbb{R}$. Therefore $(g, g) \in R$.
- **Symmetric property:** Suppose we have $(g, h) \in\ R$ then we get $\exists\ c > 0, a > 0, x > a, |g(x) - h(x)| \leq c|f(x)|$. It not hard to see that $\exists\ c > 0, a > 0, x > a, |h(x) - g(x)| \leq c|f(x)|$, for the same constants c, a. Therefore, $(h, g) \in R$.
- **Transitive property:** Suppose $(g, h) \in R$ for some constants c, a and $(h, i) \in R$ for some constants c', a'. Use triangle inequality we get:

$$\begin{aligned}|g(x) - i(x)| &= |g(x) - h(x) + h(x) - i(x)| \\ &\leq |g(x) - h(x)| + |h(x) - i(x)| \\ &\leq c|f(x)| + c'|f(x)| \\ &= (c + c')|f(x)|\end{aligned}$$

  Now for (g, i) we can just fix two positive constants $c'' = c + c'$ and $a'' = \max(a, a')$, then $(g, i) \in R$.

Since we have proved the three properties of an equivalence relation, so R is an equivalence relation. ■

Problem 4

Euler's Theorem. This is a generalization of Fermat's little theorem to nonprime moduli. Let $\phi(n)$ denote the number of integers less than n which are relatively prime to n. For example, $\phi(10) = 4$ since $1, 3, 7, 9$ are relatively prime to 10. Prove that if $a \in \mathbb{Z}$ is relatively prime to n, then

$$a^{\phi(n)} \equiv 1 \mod n$$

Hint: Consider the set $\{ia : 1 \leq i \leq n - 1, \gcd(i, n) = 1\}$ and mimic our proof of Fermat's Little Theorem.

Proof: Let $S = \{ia : 1 \leq i \leq n - 1, \gcd(i, n) = 1\} = \{i_1, i_2, \ldots, i_{\phi(n)}\}$.
Then another set $aS = \{ai_1, ai_2, \ldots, ai_{\phi(n)}\}$. Since we have a, n are relatively prime, $\gcd(a, n) = 1$. By the fact that a permutes i_l, i.e. if $ai_j \equiv ai_k \mod n$ then $j = k$, then the sets S and aS are considered as sets of congruence classes modulo n, which are identical. Hence, we could have

Problem 4 continued on next page...

$$ai_1 \cdot ai_2 \cdots ai_{\phi(n)} \equiv i_1 \cdot i_2 \cdots i_{\phi(n)} \mod n$$
$$a^{\phi(n)} \equiv 1 \mod n$$

■

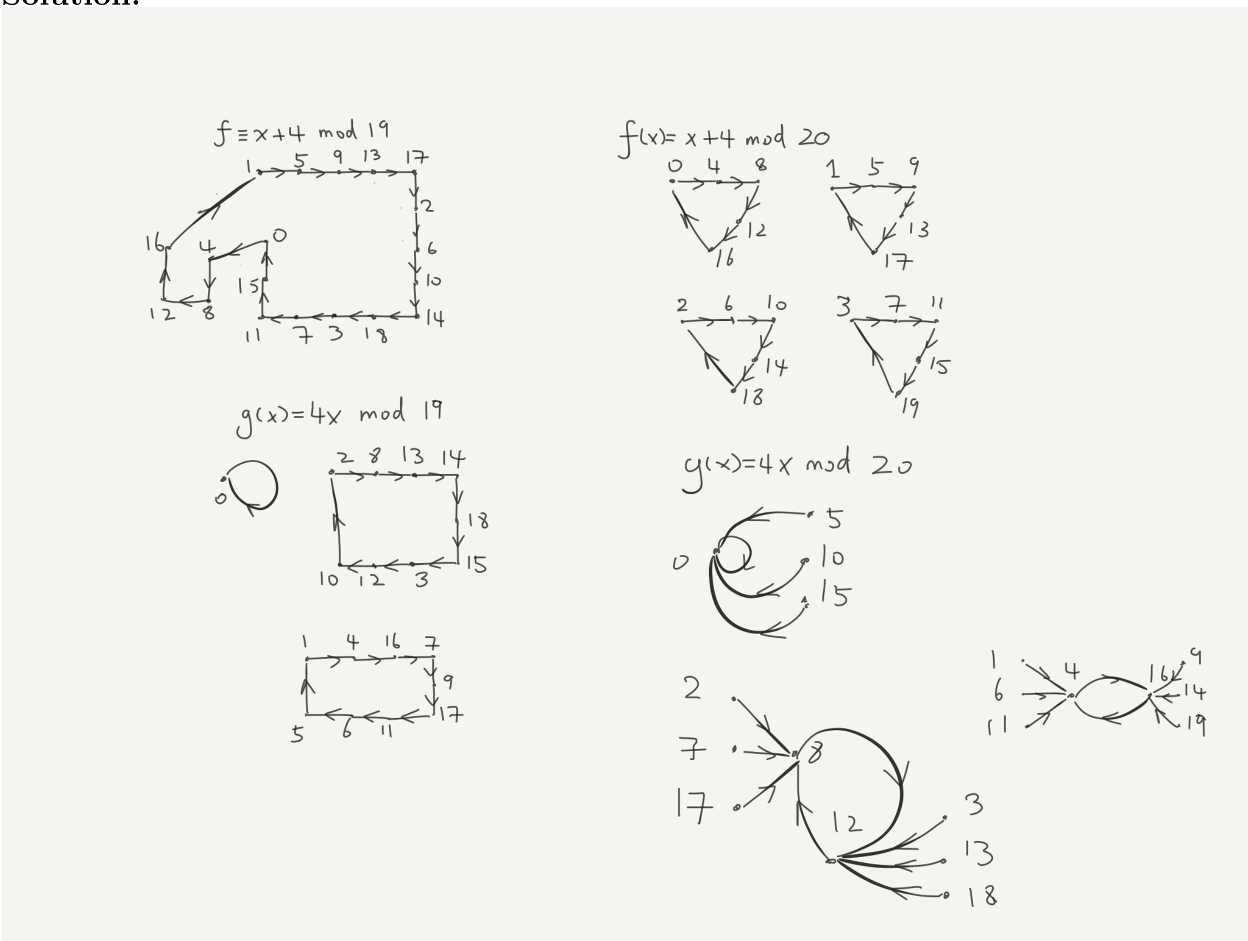
Problem 5

Functional Digraphs from Modular Arithmetic. Define f and g from $\mathbb{Z}_n$ to $\mathbb{Z}_n$ by

$$f(x) \equiv x + a \mod n$$
$$g(x) \equiv ax \mod n$$

(a) Draw the functional digraphs of f and g in the cases $(n, a) = (19, 4)$ and $(n, a) = (20, 4)$.

Solution:



(b) Give a complete description of the functional digraph of f in terms of a and n.

Solution: The functional digraph of f is a collection of $\gcd(n, a)$ cycles with length $\frac{n}{\gcd(n,a)}$.

In our case, when $n = 19, a = 4, \gcd(19, 4) = 1$, the functional digraph of f is a cycle of length $19/1 = 19$. When $n = 20, a = 4, \gcd(20, 4) = 4$, the functional digraph of f is 4 cycle of length $20/4 = 5$.

The reasoning is we would like to add multiple a's to a number in order to get a multiple of n. Such minimum multiple of n is the least common multiple of n and a, which satisfies

$$\operatorname{lcm}(n, a) = \frac{na}{\gcd(n, a)}$$

Also need to divide $\operatorname{lcm}(n, a)$ by the "step-length", which is a, so the cycle length is $\frac{na}{a \cdot \gcd(n,a)} = \frac{n}{\gcd(n,a)}$.

(c) Describe a property of the digraph of g which is true whenever n is prime and false whenever n is not prime.

Solution: When n is prime, g consists of a cycle of length 1 and other cycles of equal length.

In our case, when $n = 19$, g contains a cycle from 0 to 0 and two cycles of length 9. But this fails when $n = 20$, which is not a prime.