

CS 135
Final Examination Solutions

Professor Bloom

May 12, 2009

1. **Either complete the Definition or State the Theorem** (10 points each)

- (a) Suppose $f : A \rightarrow B$ is a function. f is **surjective** if for all $b \in B$ there is some $a \in A$ such that $f(a) = b$.
- (b) Suppose that $f : A \rightarrow B$ and $g : B \rightarrow C$ are functions. The **composite** $g \circ f : A \rightarrow C$ is the function h such that $h(a) = g(f(a))$, for all $a \in A$.
- (c) The **greatest common divisor** of two nonnegative integers, $\gcd(n, m)$, is the largest integer d which divides both n and m .
- (d) Two integers n, m are **relatively prime**, $n \perp m$, if $\gcd(n, m) = 1$.
- (e) For a positive integer n , the set \mathbb{Z}_n^* consists of the set of nonnegative integers x such that $0 \leq x < n$ and $\gcd(x, n) = 1$.
- (f) The **Euler phi-function** $\varphi(n)$ is defined as the number of elements in \mathbb{Z}_n^* .
- (g) A **permutation** $f : A \rightarrow A$ of the set A is a bijection $A \rightarrow A$.
- (h) State Euler's theorem about $a^{\varphi(n)}$.
If $a \perp n$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$
- (i) State the Chinese remainder theorem.

Suppose that n, m are positive integers and $n \perp m$. Then, for any integers a, b there is some x in the range $0 \leq x < mn$ such that

$$\begin{aligned}x &\equiv a \pmod{n} \\x &\equiv b \pmod{m},\end{aligned}$$

and if y is any integer with these two properties, then $x \equiv y \pmod{mn}$.

(j) State Wilson's theorem.

A positive integer is a prime iff $(n-1)! \equiv -1 \pmod{n}$.

2. **Examples.** (20 points each)

- (a) 1. Suppose $(2\ 4\ 7)(1\ 3)$ is the cyclic representation of the permutation $f : [8] \rightarrow [8]$, where $[8] = \{1, 2, 3, 4, 5, 6, 7, 8\}$.

Fill in the values of f below:

$$f(1) = 3 \qquad f(7) = 2 \qquad f(5) = 5.$$

Show how to write f as a composite $\tau_1\tau_2\dots$ of transpositions.

$$f = (2\ 4)(2\ 7)(1\ 3).$$

What is the f -orbit of 3?

$$(3\ 1).$$

2. Suppose $f : [5] \rightarrow [5]$ is the permutation defined by:

$$f(1) = 2; f(2) = 3; f(3) = 1; f(4) = 5; f(5) = 4.$$

What is the cyclic decomposition of f ?

$$f = (1\ 2\ 3)(4\ 5).$$

- (b) Use the Euclidean algorithm to compute $\gcd(834, 644)$ by hand.
We use: $\gcd(n, m) = \gcd(m, n \bmod m)$.

$$\begin{aligned} \gcd(644, 190) &= \gcd(190, 644 - 570 = 74) \\ &= \gcd(74, 190 - 148 = 42) \\ &= \gcd(42, 32) = \gcd(32, 10) \\ &= \gcd(10, 2) \\ &= \gcd(2, 0) = 2. \end{aligned}$$

- (c) If $p > 2$ is a prime, what are the possible values of $p \bmod 4$? Justify your answer.
Either 1 or 3, since if $p \bmod 4 = 0$, $4|p$, so p is not prime; and if $p \bmod 4 = 2$, then $4|(p-2)$ so that p is even.
- (d) Find an example of a function $f : A \rightarrow B$ and a function $g : B \rightarrow A$ such that the composite $g \circ f : A \rightarrow A$ is the identity function on A , and such that neither f nor g is the identity function.
Let $A = \{1\}$ and $B = \{1, 2\}$; define $f(1) = 2$ and $g(1) = g(2) = 1$. Then $g \circ f$ is the identity function on $\{1\}$.

3. **Coding.** (20 points each)

- (a) Suppose A, B are lists of integers which contain no integer more than once. Write code for a Scheme function (`union A B`) which returns a list (with no repetitions!) which contains all of the elements in either A or B .

```
;; join two lists
(define (union A B)
  (cond
    ((null? B) A)
    ((member? (car B) A) (union A (cdr B)))
    (else (union (cons (car B) A) (cdr B)))
  ))
```

- (b) Suppose A, B are lists of integers which contain no integer more than once. Write code for a Scheme function (`int A B`) that returns the a list with no repetitions of those elements which occur in both A and B .

```
(define (int A B)
  (cond
    ((null? B) null)
    ((member? (car B) A) (cons (car B) (int A (cdr B))))
    (else (int A (cdr B)))
  ))
```

- (c) The base 3 system to name integers assigns to any positive integer n the sequence $(x_k, x_{k-1}, \dots, x_1, x_0)$ of “ternary digits” 0,1,2 such that

$$n = x_k 3^k + x_{k-1} 3^{k-1} + \dots + x_1 3 + x_0.$$

and $x_k > 0$. Write code for a Scheme function (`base3rep n`) which, given a positive integer n returns the base 3 representation of n . For example (`base3rep 14`) returns `(1 1 2)` since $14 = 1 \cdot 3^2 + 1 \cdot 3 + 2$.

```
(define (base3rep n)
  (cond
    ((< n 3) (list n))
    (else (append (base3rep (quotient n 3)) (list (modulo n 3))))
  ))
```

- (d) Write code for a Scheme function (`1cyc f n`) which, given a permutation $f : [n] \rightarrow [n]$, returns the orbit of the least $i \in [n]$ such that $f(i) \neq i$, if i exists, and the empty list if f is the identity function.

```
(define (1cyc f n)
  (define (aux i L)
    (cond
      ((> i n) L)
      ;; now look for least i s.t. (f i) is not i
      ((= i (f i)) (aux (add1 i) L))
      ((and (not (null? L)) (= i (car L))) L)
      (else (aux (f i) (snoc i L))))
    (aux 1 null))
```

- (e) Write code for a Scheme function (`probablyprime? n`), sometimes called “Fermat prime”, which, returns either `#t` or `#f`. If it returns `#t`, then n is a prime with probability at least $1 - (1/10^6)$; if it returns `#f`, n is not prime.

We use the fact that if n is prime and $a \perp n$ then $a^{n-1} \equiv 1 \pmod{n}$, so that $a^n \equiv a \pmod{n}$. We choose 20 random ints a in the range $0, \dots, n-1$ and compute $a^n \bmod n$. If for each choice, we get $a^n \equiv a \pmod{n}$, we declare n probably prime.

```
(define (probably-prime? n)
  (define (aux count) ;
    (let (
      (a (random n))
      )
      (cond
        ((= count 20) #t); 2^20 > 10^6.
        ((= (mod^ a n n) a) (aux (add1 count)))
        ; (mod^ a p m) computes a^p mod m
        (else #f)
      )))
  (aux 0))
```

4. Problems. (20 points each)

- (a) The way we proved the equation $\varphi(nm) = \varphi(n) \times \varphi(m)$, when n, m are positive relatively prime integers is to show that, in this case (that is, when $n \perp m$), the function $f : \mathbb{Z}_{nm}^* \rightarrow \mathbb{Z}_n^* \times \mathbb{Z}_m^*$ defined by

$$f(x) := (x \bmod n, x \bmod m)$$

is a *bijection*. Is it enough to prove only that f is surjective? i.e., for any $i \in \mathbb{Z}_n^*$ and any $j \in \mathbb{Z}_m^*$, there is some $x \in \mathbb{Z}_{mn}^*$ such that $f(x) = (i, j)$? *Don't prove f is surjective*. You must decide whether

you need to prove f is injective if you have proved f is surjective. Justify your answer.

Yes, we do, since the two sets \mathbb{Z}_{mn}^ and $\mathbb{Z}_n^* \times \mathbb{Z}_m^*$ are not the same.*

- (b) Now prove f in the previous problem is surjective.

By the Chinese remainder theorem, for any pair $(i, j) \in \mathbb{Z}_n^* \times \mathbb{Z}_m^*$ there is some x in the range $0 \leq x < mn$ such that $f(x) = (i, j)$. But we have to show $x \perp mn$. If not, then some prime p divides both x and mn . Then, either $p|m$ or $p|n$, since $m \perp n$. But then, either $j = \gcd(x, m) \geq p$ or $i = \gcd(x, n) \geq p$, contradicting the fact that $i \perp n$ and $j \perp m$.

- (c) 1. Suppose n, m are integers satisfying

$$1 = 13n - 45m.$$

What can you say about $\gcd(n, m)$? Justify your answer.

$\gcd(n, m) = 1$, since any integer that divided both n and m must divide $13n - 45m = 1$.

2. Are there any integers n, m such that $1 = 12n - 45m$?

Justify your answer.

No, since 3 divides both 12 and 45.

- (d) Prove the following by induction on n . If p_i is an odd prime, for $i = 1, 2, \dots, n$, and if $p_1 p_2 \cdots p_n \equiv 3 \pmod{4}$, then for at least one value of i , $p_i \equiv 3 \pmod{4}$.

If $n = 1$ there is nothing to prove. If $n > 1$ and $p_n \not\equiv 3 \pmod{4}$, then $p_n \equiv 1 \pmod{4}$, by problem 3 in the Example section above, so that $p_1 \cdots p_{n-1} \equiv 3 \pmod{4}$. By induction, one of p_1, \dots, p_{n-1} is congruent to 3 mod 4.

- (e) What two concepts introduced in this course were the most significant, and why?