NAME: SOLUTIONS

Instructions: Check that your test has 10 pages, including this one and the blank one on the bottom. There are 8 problems on the exam. *Write neatly:* solutions deemed illegible will not be graded, so no credit will be given. You must show all work, justify all nonobvious parts of your work, and reference theorems or other facts you know from class or textbook in order to receive credit. Use English. This exam is closed book, closed notes. Calculators are not allowed.

PLEDGE: On my honor as a student, I have neither given nor received aid on this exam.

SIGNATURE: ______________________

1. (16 points) __________
2. (12 points) __________
3. (5 points) __________
4. (5 points) __________
5. (5 points) __________
6. (3 points) __________
7. (3 points) __________
8. (6 points) __________

Total (out of 55): __________

1. (2 pts each) Answer each of the following questions by circling TRUE or FALSE. You do not need to justify you answer and no partial credit will be given.

(a) $\boxed{\text{TRUE}}$ FALSE

If A and B are sets with the same power sets, then $A = B$. (section 1.6, exercise 16)

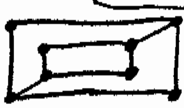
(b) TRUE $\boxed{\text{FALSE}}$

Function $f\colon \mathbf{Z} \times \mathbf{Z} \longrightarrow \mathbf{Z}$ given by $f(m, n) = |m| - |n|$ is injective. (section 1.8, ex. 15)

(c) TRUE $\boxed{\text{FALSE}}$

The coefficient of x^7 in the binomial expansion of $(1 + x)^{11}$ is $P(11, 7)$. (section 4.4, ex. 6)

(d) TRUE $\boxed{\text{FALSE}}$

Graphs  and  are isomorphic. (notes, 10/31)

(e) $\boxed{\text{TRUE}}$ FALSE

A nonplanar graph must contain K_5 or $K_{3,3}$. (notes 11/2 or Thm 2, p. 610)

(f) $\boxed{\text{TRUE}}$ FALSE

If a and b are positive integers, then $ab = gcd(a, b)lcm(a, b)$. (notes 11/7 or Thm 7, p. 161)

(g) $\boxed{\text{TRUE}}$ FALSE

17 is a factor of $8^{16} - 1$. (notes 11/14)

(h) TRUE $\boxed{\text{FALSE}}$

An inverse of a modulo m only exists if $gcd(a, m) > 1$. (section 2.6, ex. 10)

2. (3 pts each) State the following: (all were also stated in class)

(a) The Generalized Pigeonhole Principle:

See Thm 2, page 314.

(b) The Four-Color Theorem:

See Thm 1, page 614.

(c) The Fundamental Theorem of Arithmetic:

See Theorem 2, page 155.

(d) Fermat's Little Theorem:

See page 59 in Silverman.

3. (5 pts) Prove that the set of positive real numbers is uncountable.

(midterm, notes 9/14 ~~[illegible]~~, or example 20, p. 235 ~~[illegible]~~).

OK to Assume Lemma that a subset of an ~~un~~countable set is ~~un~~countable (see notes for proof).

Show $B = (0,1)$ uncountable

$\Rightarrow$ $\mathbb{R}^+$ uncountable by this lemma.

Suppose $(0,1)$ countable. Then $\exists$ a list

$a_1 = 0.\, d_{11}\, d_{12}\, d_{13} \dots$
$a_2 = 0.\, d_{21}\, d_{22}\, d_{23} \dots$
$a_3 = 0.\, d_{31}\, d_{32}\, d_{33} \dots$
$\vdots$

containing every real number in $(0,1)$.
Consider the real number

$d = 0.\, d_1\, d_2\, d_3 \dots$, where

$$d_i = \begin{cases} 4, & \text{if } d_{ii} \neq 4 \\ 5, & \text{if } d_{ii} = 4. \end{cases}$$

d is <u>not</u> on the list since the expansion of d differs from expansion of a_i in slot i $\forall i$.

4. (5 pts) Show that the relation on $\mathbf{Z} \times \mathbf{Z}$ given by $R = \{(a, b) \mid a \equiv b \ (m)\}$ is an equivalence relation.

(see notes 10/22 or exercise 4, p. 509)

R is reflexive: $a \equiv a \ (m) \quad \forall a \in \mathbb{Z}$ since $m \mid (a-a) = 0$.

Symmetric: $a \equiv b \ (m) \Rightarrow b \equiv a \ (m)$

because if $m \mid a-b$, then $m \mid -(a-b) = b-a$, i.e. $b \equiv a \ (m)$.

transitive: If $a \equiv b \ (m)$ and $b \equiv c \ (m)$, that means $a - b = km$ for some $k \in \mathbb{Z}$, and $b - c = lm$ for some $l \in \mathbb{Z}$.

Adding these equations, get

$a - c = (k + l) m$

$\Rightarrow a \equiv c \ (m)$.

5. (5 pts) Prove that there are infinitely many primes.

(See notes 11/7 or Thm 4, p. 156)

Assume there are finitely many, say

$p_1, p_2, \ldots, p_n$.

Let $P = p_1 p_2 \cdots p_n + 1$

Then P is either prime, in which case we are done (by contradiction, since P is different from all p_i's), or it is composite so it must be divisible by 2 or more primes $p_1, p_2, \ldots, p_n$.

But if $p_i \mid P$ for some i,

and $p_i \mid p_1 p_2 \cdots p_i \cdots p_n$, then

$$p_i \mid (P - p_1 p_2 \cdots p_i \cdots p_n) = 1 .$$

But this is a contradiction.

6. (3 pts) Reduce 3^{563} modulo 11.

(see notes 11/9)

Use $3^{10} \equiv 1 \ (11)$ (Fermat's little Theorem)

so $3^{563} = (3^{10})^{56} \cdot 3^{3} \equiv 1^{56} \cdot 3^{3} \ (11)$

$\equiv 27 \ (11) \equiv \boxed{5 \ (11)}$

7. (3 pts) Find ~~$\phi(97)$~~. $\phi(220)$.

Since $220 = 2^2 \cdot 5 \cdot 11$,

$$\phi(220) = \phi(2^2 \cdot 5 \cdot 11) = \phi(2^2)\phi(5)\phi(11)$$

$$= (2^2 - 2) \cdot 4 \cdot 10 = \boxed{80.}$$

(This is like exercise 11.1 in Silverman) from notes, 11/30.

8. (6 pts) Describe the encryption and decryption procedure in the RSA cipher. In other words, write down how, starting with plaintext P, one obtains the ciphertext C, and vice versa. Make sure to clearly identify the public and private keys.

Choose p, q prime. Let $n = pq$. Find $\phi(n) = (p-1)(q-1)$

Choose e such that $\gcd(e, \phi(n)) = 1$.

To encrypt: Translate letters of message into their # equivalents (e.g. $A = 11$, $B = 12$, ..., $Z = 36$).

Divide into blocks whose length is $< n$.

Encrypt each block P by

$$C \equiv P^e \ (n)$$

So public key is (e, n).

To decrypt: Find inverse of e mod $\phi(n)$. (This exists since $\gcd(e, \phi(n)) = 1$). Call it d.

Then, given C,

$$P \equiv C^d \ (n).$$

So private key is d (or $\phi(n)$, or n, since without those, d is practically impossible to find for large p and q).