Key

Final Exam

Math 258
(Spring 2006)

Solve the following problems. Show all your work in the space under each problem.

1. (a) Show that if $n \in \mathbf{Z}$ is a composite, then n has a prime divisor $\leq \sqrt{n}$. (18 pts)

n comp. $\Rightarrow n = ab$, $1 < a, b < n$

Must be $a \leq \sqrt{n} \vee b \leq \sqrt{n}$, bec. otherwise $a > \sqrt{n} \wedge b > \sqrt{n} \Rightarrow ab > n$ ↯

If, say a, is prime, then n has a prime divisor (that is a) $\leq \sqrt{n}$

If a is not prime, then a has a prime divisor, which is also a divisor of n and $\leq \sqrt{n}$.

(b) Use the above to examine whether 131 is prime.

The only primes $\leq \sqrt{131}$ are: 2, 3, 5, 7, 11

From these, none divides 131

Hence 131 is prime.

(c) Show that there are infinitely many primes

Assume $\exists$ fin. many primes, say $p_1, p_2, \ldots, p_n$

Consider the number $p_1 p_2 \cdots p_n + 1$

Then, this number should be either prime or composite.

If it's prime, then since is $>$ than any of the p_i's above it is not one of the primes in the list ↯

If it's comp., then it has a prime divisor p_j (p_j from the list)

Since $p_j \mid p_1 p_2 \cdots p_n + 1 \wedge p_j \mid p_1 p_2 \cdots p_n \Rightarrow p_j \mid 1$ ↯

(d) **True** or **False**: If p is prime, then $p! + 1$ is prime.

False, take $p = 5$.

Then, $5! + 1 = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 + 1 = 121$ which is not prime $(121 = 11 \cdot 11)$

(e) If $p_1, p_2, \ldots, p_n$ are the first n consecutive primes, does it necessarily imply that $p_1 p_2 \cdots p_n + 1$ is prime?

No, consider $1 \cdot 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30030 + 1$

$= 30031$

$= 59 \cdot 509$ → ie composite

(f) The function $f(n) = n^2 - n - 1$, $n > 2$, fails to be a prime-generating function for:

A. $n = 6$ B. $n = 10$ C. $n = 12$ (D.) $n = 13$

$f(13) = 13^2 - 13 - 1$

$= 169 - 13 - 1$

$= 155$

but 155 is not prime

$(155 = 31 \cdot 5)$

2. (a) Define the **gcd(*a*,*b*)** and **lcm(*a*,*b*)** , for $a, b \in \mathbf{Z}-\{0\}$. (10 pts)

- Let $a,b \in \mathbb{Z}$. The largest $d \in \mathbb{Z}_{>0}$ st $d|a$ and $d|b$ is called the greatest common divisor of a and b. We denote it by $\gcd(a,b)$.
- Let $a,b \in \mathbb{Z}$. The smallest $m \in \mathbb{Z}_{>0}$ st $a|m$ and $b|m$ is called the least common multiple of a and b. We denote it by $\text{lcm}(a,b)$.

(b) Appropriate formula for lcm(*a*,*b*) gives that the lcm$(3^2 \cdot 5 \cdot 7^2 \cdot 11 \, , \, 2 \cdot 3 \cdot 7^3)$ is:

A. $3^2 \cdot 5 \cdot 7^2 \cdot 11 \cdot 2 \cdot 3 \cdot 7^3$ B. $3 \cdot 7^2$ (C.) $2 \cdot 3^2 \cdot 5 \cdot 7^3 \cdot 11$ D. $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$

$$\text{lcm}(3^2 5 \cdot 7^2 \cdot 11, 2 \cdot 3 \cdot 7^3) = 2^{\max(0,1)} 3^{\max(2,1)} 5^{\max(1,1)} 7^{\max(3,1)} 11^{\max(1,0)}$$
$$= 2^1 \cdot 3^2 \cdot 5^1 \cdot 7^3 \cdot 11^1$$

3. (a) Show that if the gcd(*a*,*m*) > 1, then *a* has **no** inverse in $\mathbb{Z}_m$ (12 pts)

Assume a has an inverse in $\mathbb{Z}_m$. Say b.
Then, $ab = 1$ in $\mathbb{Z}_m$, or $ab \equiv 1 \bmod m$. The latter implies $ab = 1 + km$.
Let $\gcd(a,m) = d > 1$. Then, $d|a \wedge d|m \Rightarrow d|ab \wedge d|km \Rightarrow d|1$ ↯.

(b) Use the *extended Euclidean algorithm* to write the gcd(87,38) as a linear combination of 87 and 38. Use that relation to find the inverse of 38 in $\mathbb{Z}_{87}$.

The Eucl. Alg. gives :

$87 = 2 \cdot 38 + 11$
$38 = 3 \cdot 11 + 5$
$11 = 2 \cdot 5 + \boxed{1}$
$5 = 1 \cdot 5 + 0$

ie, $\gcd(87,38) = 1$

The Ext. Eucl. Alg. gives :

$1 = 1 \cdot 11 - 2 \cdot 5$
$1 = 1 \cdot 11 - 2 \cdot (38 - 3 \cdot 11)$
$1 = 7 \cdot 11 - 2 \cdot 38$
$1 = 7(87 - 2 \cdot 38) - 2 \cdot 38$
$1 = 7 \cdot 87 - 16 \cdot 38$

Since $1 = 7 \cdot 87 + (-16) \cdot 38$ and $87 = 0$ in $\mathbb{Z}_{87}$, then $38^{-1} = -16 = 71$

4. (a) Show that if *a*, *b*, *k* and *m* are integers such that $a \equiv b \bmod m$ and $k \geq 1$, $m \geq 2$, then $a^k \equiv b^k \bmod m$. (15 pts)

(*Hint*: Use the identity for $a^k - b^k$).

We know that $a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + \cdots + a^{k-\lambda-1}b^{\lambda} + \cdots + ab^{k-2} + b^{k-1})$
Since $a \equiv b \bmod m \Rightarrow m|a-b$, which implies that $m|(a-b)(\gg)$
ie, $m|a^k - b^k$.

(b) Is the converse true? Examine the case for $k = 2$.

No, consider the case $k=2$, $a=4$, $b=3$, $m=7$. Then, $4^2 \equiv 3^2 \bmod 7$ but $4 \not\equiv 3 \bmod 7$

(c) A solution to the congruency $8x \equiv 2 \bmod 13$ is:

A. $x \equiv 2 \bmod 13$ B. $x \equiv 7 \bmod 13$ (C.) $x \equiv 10 \bmod 13$ D. $x \equiv 13 \bmod 13$

$8^{-1} = 5$ in $\mathbb{Z}_{13}$. So, $5 \cdot 8x \equiv 5 \cdot 2 \bmod 13 \Rightarrow x \equiv 10 \bmod 13$

5. Show that $\binom{2n}{2} = 2\binom{n}{2} + n^2$, where $n \in \mathbf{N} - \{0\}$. (10 pts)

$$\text{LHS} = 2\binom{n}{2} + n^2 = 2\frac{n!}{2!(n-2)!} + n^2$$
$$= (n-1)n + n^2$$
$$= 2n^2 - n$$
$$= n(2n-1) = \frac{2n(2n-1)}{2} = \frac{2n(2n-1)(2n-2)!}{2(2n-2)!} = \binom{2n}{2}$$

6. (a) What is the probability that a five-card poker hand does not contain the queen of hearts? (10 pts)

$$P(E) = \frac{\binom{51}{5}}{\binom{52}{5}} = \frac{47}{52}$$

(b) What is the probability to roll a 2 in a 3-number biased die, in which 1 is three times as likely to come up as 3 and 2 is two times as likely to come up as 3?

$$\left.\begin{aligned} P(1) &= 3P(3) \\ P(2) &= 2P(3) \\ P(1)+P(2)+P(3) &= 1 \end{aligned}\right\} \Rightarrow \frac{3P(2)}{2} + P(2) + \frac{P(2)}{2} = 1 \Rightarrow \frac{6P(2)}{2} = 1$$
$$\Rightarrow P(2) = 1/3$$

7. A relation R on a set A is called **irreflexive** if $(x \in A \Rightarrow (x,x) \notin A, \forall x \in A)$. In other words, no element in A relates to itself. Suppose now that a relation R is irreflexive. Is R^2 necessarily irreflexive? Explain. (5 pts)

No, consider $R = \{(1,2),(2,1)\}$, on $A = \{1,2\}$, which is irreflexive.
Then, $R^2 = \{(1,1),(2,2)\}$ is not irreflexive.

8. (a) Determine whether the following relation on the set of all functions from **Z** to **Z** is an equivalence relation. Make sure you check all the relevant properties: (10 pts)

$$R = \{(f,g) \mid f(x) - g(x) = C, \text{ for some } C \in \mathbf{Z}, \forall x \in \mathbf{Z}\}$$

- $(f,f) \in R$, bec. $f(x) - f(x) = 0 \in \mathbb{Z}$, $\forall x$, ie R is reflexive
- If $(f,g) \in R \Rightarrow f(x) - g(x) = C$
  $\Rightarrow g(x) - f(x) = -C$, $C' \in \mathbb{Z}$, ie R is symmetric
- If $(f,g) \in R$, $(g,h) \in R$ $\Rightarrow$ $f(x) - g(x) \in C$, $g(x) - h(x) \in C'$ $\overset{(+)}{\Rightarrow}$ $f(x) - h(x) = C + C'$, $C'' \in \mathbb{Z}$, ie R is transitive

Hence, R is an equiv. re

(b) What is the equivalence class of $f(x) = x^2$?

$$[x^2] = \{g \mid x^2 - g(x) = C\}$$
$$= \{g \mid g(x) = x^2 - C\}$$
$$= \{x^2 - C, \text{ some } C \in \mathbb{Z}\}$$

9. (a) Find the equivalence relation induced by the following partition of the set $S = \{0,1,2,3,4,5\}$: (10 pts)

$$\{0\}, \{1,2\}, \{3,4,5\}.$$

$R = \{(0,0), (1,2), (2,1), (1,1), (2,2), (3,4), (4,3),$
$(3,3), (4,4), (3,5), (5,3),$
$(5,5), (4,5), (5,4)\}$

(b) Are the elements 1 and 4 equivalent?

No, bec. 1 and 4 belong to different equiv. classes.
$(1 \in \{1,2\}, 4 \in \{3,4,5\})$