Final Exam

Math 258
(Fall 06)

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 $\leq \sqrt{n}$. (25 pts)

n composite $\Rightarrow n = ab$, $1 < a, b < n$
Must be $a \leq \sqrt{n} \vee b \leq \sqrt{n}$, bec. otherwise if $a > \sqrt{n} \wedge b > \sqrt{n} \Rightarrow ab > n$ ↯
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 101 is prime.

The only primes $\leq \sqrt{101}$ are: 2, 3, 5, 7
From these, none divides 101, hence 101 is prime. //

(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 <u>not</u> a 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 $1 \cdot 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30030 + 1$
$= 30031$
$= 59 \cdot 509$, which is 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) $n = 13$

$f(13) = 13^2 - 13 - 1$
$= 169 - 13 - 1$
$= 155$, which is not a prime $(155 = 5 \cdot 31)$ //

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

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

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

3. (a) Show that if the gcd$(a,m) > 1$, then a has **no** inverse in $\mathbf{Z}_m$ (20 pts)

Assume that a has an inverse in $\mathbb{Z}_m$, say b.
Then, $ab = 1$ in $\mathbb{Z}_m$, ie $ab \equiv 1 \bmod m \Rightarrow ab = 1 + km$.
Let $\gcd(a,m) = d > 1$. Then, $d \mid a \wedge d \mid m \Rightarrow d \mid ab \wedge d \mid km \Rightarrow d \mid ab - km$
$\Rightarrow d \mid 1$ ↯ //

(b) Use the *extended Euclidean algorithm* to write the **gcd**(35, 78) as a linear combination of 35 and 78. Use that relation to find the inverse of 35 in Z_{78}.

The Eucl. Alg. gives : $78 = 2\cdot 35 + 8$, $35 = 4\cdot 8 + 3$, $8 = 2\cdot 3 + 2$, $3 = 1\cdot 2 + \boxed{1}$, $2 = 1\cdot 2 + 0$

ie, $\gcd(35,78) = 1$

The Ext. Eucl. Alg. gives :

$1 = 3 - 1\cdot 2$

$1 = 3 - 1\cdot(8 - 2\cdot 3)$

$1 = 3\cdot 3 - 1\cdot 8$

$1 = 3(35 - 4\cdot 8) - 1\cdot 8$

$1 = 3\cdot 35 - 13\cdot 8$

$1 = 3\cdot 35 - 13(78 - 2\cdot 35) = 29\cdot 35 - 13\cdot 78$

Since $1 = 29\cdot 35 + (-13)78$ and $78 = 0$ in Z_{78}, then $35^{-1} = 29$ //

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 $a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + \dots + a^{k-j-1}b^j + \dots + ab^{k-2} + b^{k-1})$

Since $a \equiv b \bmod m \Rightarrow m \mid a-b$

$\Rightarrow m \mid (a-b)(\gg) \Rightarrow m \mid a^k - b^k$ //

(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 $3x \equiv 4 \bmod 7$ is:

A. $x \equiv 12 \bmod 7$ B. $x \equiv 5 \bmod 7$ (C.) $x \equiv 6 \bmod 7$ D. $x \equiv 4 \bmod 7$

$3^{-1} = 5$ in Z_7. So, $5\cdot 3x = 5\cdot 4 \bmod 7 \Rightarrow 1\cdot x = 20 \bmod 7$

$\Rightarrow x = 6 \bmod 7$ //

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

$RHS = 2\binom{n}{2} + n^2 = 2\cdot \frac{n!}{2!(n-2)!} + n^2$

$= (n-1)n + n^2$

$= 2n^2 - n$

$= n(2n-1) = \frac{2n(2n-1)}{2} = \frac{2n(2n-1)(2n-2)!}{2(2n-2)!} = \binom{2n}{2}$ //

6. 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? (5 pts)

$P(1) = 3P(3)$

$P(2) = 2P(3)$

$P(1) + P(2) + P(3) = 1$

$\Rightarrow \frac{3P(2)}{2} + P(2) + \frac{P(2)}{2} = 1$

$\Rightarrow \frac{6P(2)}{2} = 1$

$\Rightarrow P(2) = 1/3$ //

7. (a) Determine whether the following relation on the set of all functions from $\mathbf{Z}$ to $\mathbf{Z}$ is an equivalence relation. Make sure you check all the relevant properties: (10 pts)

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

(i) $(f,f) \in R$, bec. $f(x) - f(x) = 0 \in \mathbb{Z}$, $\forall x$, ie R reflexive

(ii) If $(f,g) \in R \Rightarrow f(x) - g(x) = C$

$\Rightarrow g(x) - f(x) = \underbrace{-C}_{C'} \in \mathbb{Z} \quad \forall x$

$\Rightarrow (g,f) \in R$, ie R symmetric

(iii) If $\left.\begin{matrix}(f,g) \in R \\ (g,h) \in R\end{matrix}\right\} \Rightarrow \begin{matrix} f(x) - g(x) = C \\ g(x) - h(x) = C' \end{matrix} \overset{(+)}{\Rightarrow} f(x) - h(x) = \underbrace{C + C'}_{C''} \in \mathbb{Z}$

$\Rightarrow (f,h) \in R$

ie, R transitive.

Hence, R is an equiv. rel.

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

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

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

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

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

(b) Are the elements 2 and 5 equivalent?

No, bec. 2 and 5 belong to different equiv. classes.

$(2 \in \{2,3\}, 5 \in \{4,5\})$ //