

TEST 3 - Key

(Math 258 B)

1. (a) Show that if a divides b , then a^2 divides b^2

$$\begin{aligned} a \mid b &\Rightarrow b = ka \\ &\Rightarrow b^2 = k^2 a^2 \\ &\Rightarrow b^2 = \lambda a^2, \text{ where } \lambda = k^2 \\ &\Rightarrow a^2 \mid b^2 \end{aligned}$$

(b) Prove or disprove: If p and q are primes, then $p^2 + q^2$ is a prime

Disprove by counter example:

$$\text{Let } p = 3 \text{ and } q = 5$$

$$\begin{aligned} \text{Then, } p \text{ and } q \text{ are prime, but } p^2 + q^2 &= 3^2 + 5^2 \\ &= 9 + 25 \\ &= 34, \text{ but } 34 \text{ is not prime} \end{aligned}$$

(c) Show that if a^2 is even, then it is divisible by 4

$$\begin{aligned} a^2 \text{ even} &\Rightarrow a \text{ even} \\ &\Rightarrow a = 2k \\ &\Rightarrow a^2 = 4k^2 \\ &\Rightarrow 4 \mid a^2 \end{aligned}$$

2. Find the prime factorization of 1001.

We start dividing 1001, and its quotients, with primes:

$$1001 / 7 = 143$$

$$143 / 11 = 13$$

13 is prime, so stop

$$\text{Hence, } 1001 = 7 \cdot 11 \cdot 13$$

3. Find the gcd(a,b) and the lcm(a,b) of the following integers.

$$a = 2^3 \cdot 3^2 \cdot 7 \cdot 11^2 \cdot 17^2 \quad \text{and} \quad b = 2^2 \cdot 3^4 \cdot 5 \cdot 11$$

$$\mathbf{gcd(a, b) = 2^2 \cdot 3^2 \cdot 11}$$

$$\mathbf{lcm(a,b) = 2^3 \cdot 3^4 \cdot 5 \cdot 7 \cdot 11^2 \cdot 17^2}$$

4. Use the *extended Euclidean algorithm* to write the gcd(277, 123) as a linear combination of 277 and 123. Use that relation to find the inverse of 123 in Z_{277} .

$$277 = 2 \cdot 123 + 31$$

$$123 = 3 \cdot 31 + 30$$

$$31 = 1 \cdot 30 + 1$$

$$30 = 30 \cdot 1 + 0$$

Hence, $\mathbf{gcd(277, 123) = 1}$.

$$1 = (1)31 + (-1)30$$

$$1 = (1)31 + (-1)(123 - 3 \cdot 31)$$

$$1 = (4)31 + (-1)123$$

$$1 = (4)31 + (-1)123$$

$$1 = (4)(277 - 2 \cdot 123) + (-1)123$$

$$1 = (4)277 - (8)123 + (-1)123$$

$$1 = (4)277 + (-9)123$$

Since $277 = 0$ in Z_{277} , the last equation gives: $1 = (-9) \cdot 123$, i.e. $123^{-1} = -9$.

5. Show that if a is an odd integer, then $a^2 \equiv 1 \pmod{8}$.

$$a \text{ odd} \Rightarrow a = 2k + 1$$

$$\Rightarrow a^2 = (2k + 1)^2 = 4k^2 + 4k + 1$$

$$\Rightarrow a^2 - 1 = 4k^2 + 4k = 4k(k + 1)$$

Since k and $k+1$ consecutive, one of them is even, say k , then $k = 2\lambda$

$$a^2 - 1 \Rightarrow 4(2\lambda)(k + 1)$$

$$\Rightarrow 8\lambda(k + 1)$$

$$\Rightarrow 8 \mid a^2 - 1$$

6. Solve the congruence $4x \equiv 5 \pmod{9}$. List at least three integers that are solutions to the congruence.

The inverse of 4 in \mathbb{Z}_9 is 7. Indeed, $4 \cdot 7 = 28 = 1 + 3 \cdot 9 = 1 + 3 \cdot 0 = 1$

So,

$$7 \cdot 4x \equiv (7 \cdot 5) \pmod{9} \Rightarrow x \equiv 35 \pmod{9} \Rightarrow x \equiv 8 \pmod{9}$$

Hence, 8 is a solution. Another two solutions are: 17 and 26. As a matter of fact, all numbers of the form $8 + 9k$, $k \in \mathbb{Z}$, are solutions.

7. Solve the system of congruences:

$$\begin{aligned}x &\equiv 2 \pmod{3} \\x &\equiv 1 \pmod{4} \\x &\equiv 3 \pmod{5}\end{aligned}$$

$$m = 3 \cdot 4 \cdot 5 = 60$$

and

$$M_1 = 60 / 3 = 20$$

$$M_2 = 60 / 4 = 15$$

$$M_3 = 60 / 5 = 12$$

Then,

- 2 is the inverse of 20 modulo 3
- 3 is the inverse of 15 modulo 4
- 3 is the inverse of 12 modulo 5

The solution for of the system is: $x = 2 \cdot 20 \cdot 2 + 1 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3 = 233 \equiv 53 \pmod{60}$.