Math 104A, Midterm

Monday, May 5th, 2014, 10-10:50am, in-class, Peterson Hall 103

- *Your Name*: SOLUTIONS.

Problem 1. You are given two positive integers with prime factorizations:

$$2^4 \cdot 3^7 \cdot 7 \cdot 13^5 \quad \text{and} \quad 3 \cdot 5^5 \cdot 7^2 \cdot 11^9.$$

Find[1] the prime factorizations of their GCD, and of their LCM.

By (1.7) on p. 25,

- $GCD = 2^0 \cdot 3^1 \cdot 5^0 \cdot 7^1 \cdot 11^0 \cdot 13^0 = 3 \cdot 7 = 21$
- $LCM = 2^4 \cdot 3^7 \cdot 5^5 \cdot 7^2 \cdot 11^9 \cdot 13^5$

(take max and min of the exponents).

[1] GCD=greatest common divisor, LCM=least common multiple

Problem 2.

(a) Find the GCD and LCM of 70 and 15.

(b) Using Euclid's algorithm, find *a* pair of integers (x, y) such that

$$\mathrm{GCD}(70, 15) = 70x + 15y.$$

(c) Find *all* pairs of integers (x, y) such that $\mathrm{GCD}(70, 15) = 70x + 15y$.

(d) Show that 3 is invertible modulo 14, and compute its inverse.

(a) Euclid's algorithm:

$$70 = 4 \cdot 15 + 10$$
$$15 = 1 \cdot 10 + 5 \quad \leftarrow \mathrm{GCD}(70,15)$$
$$10 = 2 \cdot 5$$

(alternatively, $15 = 3 \cdot 5$ and $70 = 2 \cdot 5 \cdot 7$)

(b) Above eqns. give: $5 = \mathrm{GCD}(70,15) = 15 - 10$
$= 15 - (70 - 4 \cdot 15)$
$= 5 \cdot 15 + (-1) \cdot 70.$

So, a solution is
$(x,y) = (-1, 5)$

(c) Note: $5 = 70x + 15y \iff 1 = 14x + 3y \quad (\star)$ (div. by 5)

14, 3 coprime.

Recall Thm 5.1, p. 213:

$(x,y) = (-1 + 3t, 5 - 14t)$, $t \in \mathbb{Z}$
is the general solution to $(\star)$

(d) Reading $(\star)$ modulo 14, $[3]$ is invertible in $\mathbb{Z}/14\mathbb{Z}$ with inverse $[5]$.

(check: $3 \cdot 5 \equiv 1 \pmod{14}$)

Problem 3.

(a) Find a primitive Pythagorean triple (x, y, z) with hypotenuse $z = 41$.

(b) Is there a primitive Pythagorean triple (x, y, z) with $z = 43$?

(a) May assume (by interchanging x and y) that y is even, in which case we know (Thm 5.5, p. 232):

$$(x,y,z) = (m^2-n^2,\ 2mn,\ m^2+n^2).$$

m, n coprime, opposite parity.

Thus we try to write:

$$41 = m^2+n^2$$

By trial and error, find: $41 = 25+16 = 5^2+4^2$

Take $m=5$, $n=4$; which yields:

$$(x,y,z) = (9, 40, 41)$$

(the only one up to $x \leftrightarrow y$, and signs.)

(b) <u>No</u>. As above, one would have: $43 = m^2+n^2$.

Can't happen: $m \equiv 0,1,2,3 \pmod 4$

$m^2 \equiv 0,1,0,1 \pmod 4$.

$$\Rightarrow m^2+n^2 \equiv 0,2 \pmod 4.$$

But, $43 \equiv 3 \pmod 4$.

Problem 4. Let p be a prime. Prove p divides each of the binomial[2] coefficients:

$$\binom{p}{1}, \binom{p}{2}, \binom{p}{3}, \quad \ldots \quad, \binom{p}{p-1}.$$

From the footnote, we read off:

$$k! \cdot \binom{p}{k} = \underbrace{p(p-1)(p-2)\cdots(p-k+1)}_{\text{clearly divisible by } p}.$$

(as long as k is in the range $0<k<p$.)

Thus, by primality,

$p \mid k!$ or $p \mid \binom{p}{k}$.

However, $k! = 1 \cdot 2 \cdot 3 \cdots k$ (all factors $<p$) – so by another application of primality: $p \nmid k!$

Ergo, $p \mid \binom{p}{k}$ as desired.

[2] Recall that $\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{1}{k!}p(p-1)(p-2)\cdots(p-k+1)$

Problem 5. Circle the numbers divisible by 4:

435272846532, 325472714614, 4314252671, 3212425363752.

(Hint: 10^n is divisible by 4 for all $n > 1$.)

– the first number is:

$$\underbrace{2 + 3\cdot 10}_{=\,32} + \underbrace{5\cdot 10^2 + 6\cdot 10^4 + 4\cdot 10^5 + \cdots + 4\cdot 10^{12}}_{\text{divisible by 4 (since } 100 = 4\cdot 25)}$$

We just have to check whether $4 | 32$? It does.
Similarly for the other numbers — just look at the <u>last</u> <u>two</u> <u>digits</u>.