P. Set 4 Solutions

Math 42
Fall 2015

① Below are the primes up to 100. ~~for~~ sorted by congruence class.

0 mod 9	
1 mod 9	19, 37, 73
2 mod 9	2, 11, 29, 47, 83
3 mod 9	3
4 mod 9	13, 31, 67
5 mod 9	5, 23, 41, 59
6 mod 9	
7 mod 9	7, 43, 61, 79, 97
8 mod 9	17, 53, 71, 89

There are at least two in each class except 0 mod 9, 3 mod 9, & 6 mod 9. In fact, these classes have no primes except 3 itself, because any such prime would satisfy $p \equiv 0, 3,$ or $6 \bmod 3$, i.e. $p \equiv 0 \bmod 3$ and $3 | p$. So 3 is the only such prime.

② a) $55x \equiv 30 \bmod 625$

$\iff 11x \equiv 6 \bmod 125$

Using the Euclidean algorithm:

$[4] = (125) - 11\cdot(11)$

$[3] = \cancel{[4]}\,(11) - 2\cdot[4] = 23\cdot(11) - 2\cdot(125)$

$[1] = [4] - [3] = 3\cdot(125) - 34\cdot(11)$

Hence $-34\cdot 11 \equiv 1 \bmod 125$. So

$x \equiv -34\cdot 6 \bmod 125$

i.e. $x \equiv -204 \equiv 46.$

so the solutions can be expressed either by

$$\boxed{x \equiv 46 \bmod 125} \quad \text{or} \quad \boxed{x \equiv 46,\ 171,\ 296,\ 421, \text{ or } 546 \bmod 625}$$

b) Since 11 divides 1331 and 55 but not 30, this congruence has $\boxed{\text{no solutions}}$.

③ a) Suppose that y_1, y_2 are both inverses of x modulo 24. Then consider the number $y_1 x y_2$. On the one hand

$$y_1 x y_2 \equiv y_1 \cdot (x y_2) \equiv y_1 \bmod 24$$

but on the other

$$y_1 x y_2 \equiv (y_1 x) y_2 \equiv y_2 \bmod 24.$$

Hence $y_1 \equiv y_2 \bmod 24$ (both are congruent to $y_1 x y_2$).

b) Notice that if $xy \equiv 1 \bmod 24$, then $\gcd(x, 24)$ must divide 1, hence $\gcd(x, 24) = 1$.
Conversely, if $\gcd(x, 24) = 1$, then the equation $xy + 24z = 1$ has a solution (y, z), and y is an inverse of x modulo 24.
So <u>x has an inverse if and only if $\gcd(x, 24) = 1$</u>, i.e. if and only if x is not divisible by 2 or 3.

So we must find inverses for 1, 5, 7, 11, 13, 17, 19, and 23.

Each can be found with the Euclidean algorithm.

(24) (5)

$[4] = (24) - 4(5)$

$[1] = (5) - [4]$

$= 5(5) - (24).$

so 5's inverse is 5.

(24) (7)

$[3] = (24) - 3(7)$

$[1] = (7) - 2[3]$

$= 7(7) - 2(24)$

so 7's inverse is 7.

(24) (11)

$[2] = (24) - 2(11)$

$[1] = (11) - 5[2]$

$= 11(11) - 5(24)$

so 11's inverse is 11.

(24) (13)

$[11] = (24) - (13)$

$[2] = (13) - [11]$

$= 2\cdot(13) - (24)$

$[1] = [11] - 5[2]$

$= 6\cdot(24) - 11\cdot(13)$

so 13's inverse is -11 (or 13).

At this point, we can save some work by noticing that if $xy \equiv 1$, then $(-x)(-y) \equiv 1$. Since $13 \equiv -11$, $17 \equiv -7$, ~~and~~ $19 \equiv -5$ and $23 \equiv -1$, we can find the inverses of these from earlier work. ~~Note~~

x	1	5	7	11	13	17	19	23
inverse	1	5	7	11	13 ~~(or −11)~~	17	19	23.

So mod 24 arithmetic has a strange property: each invertible element is its own inverse.

(4) a) Let $L = \mathrm{lcm}(a,b)$. Suppose $\gcd(a,b)=1$. Then for some x, y.

$$ax + by = 1$$
$$\Rightarrow axL + byL = L$$
$$\Rightarrow L = ab\cdot\left(x\cdot\frac{L}{b} + y\cdot\frac{L}{a}\right)$$

so L is a multiple of ab. Since ab is a common multiple of a & b, it can't be strictly smaller than L; hence $L = ab$.

b) Suppose that N is a common multiple of ka and kb. Then $\frac{N}{k}$ is divisible by both a and b. Hence $\frac{N}{k}$ is a common multiple of a and b, so $N/k \geq \mathrm{lcm}(a,b)$, so $N \geq k\cdot\mathrm{lcm}(a,b)$. This shows that if $k\cdot\mathrm{lcm}(a,b)$ is a common multiple of ka and kb, then it must necessarily be the least one.

Now, $k\cdot\mathrm{lcm}(a,b)/(ka) = \mathrm{lcm}(a,b)/a$ and $k\cdot\mathrm{lcm}(a,b)/(kb) = \mathrm{lcm}(a,b)/b$, so $k\cdot\mathrm{lcm}(a,b)$ is a common multiple of ka, & kb. By the previous paragraph, it is equal to the least common multiple.

c) Let $g = \gcd(a,b)$. Then $\gcd\left(\frac{a}{g}, \frac{b}{g}\right) = 1$ since $\frac{a}{g}x + \frac{b}{g}y = 1$ has a solution. By part (a), $\mathrm{lcm}\left(\frac{a}{g}, \frac{b}{g}\right) = \frac{ab}{g^2}$. So by part (b),

$$\mathrm{lcm}(a,b) = g\cdot\mathrm{lcm}\left(\frac{a}{g}, \frac{b}{g}\right) = g\cdot\frac{ab}{g^2} = \frac{ab}{g}.$$

Therefore $g\cdot\mathrm{lcm}(a,b) = ab$, as claimed.

(5) The numbers (a, b, c^2) must be a primitive Pythagorean triple. So we want integers s, t, odd and with no common factors, such that

$$a = st$$
$$b = \tfrac{1}{2}(s^2 - t^2)$$
$$c^2 = \tfrac{1}{2}(s^2 + t^2) \quad \text{i.e.} \quad 2c^2 = s^2 + t^2.$$

Using PSet 2, problem 3(b), one option is $s = 7, t = 1$, since then $c = 5$ gives $2c^2 = s^2 + t^2$.

So $\underline{a = 7 \quad b = 24, \quad c = 5}$ is one solution.

Other solutions to the eqn. $2c^2 = s^2 + t^2$ from HW2 give more solutions to $a^2 + b^2 = c^4$. For example,

$$2 \cdot 13^2 = 17^2 + 7^2$$

gives the ~~solution~~ values $s = 17, t = 7$, hence

$$a = 17 \cdot 7 = 119$$
$$b = \tfrac{1}{2}(17^2 - 7^2) = 120$$
$$c = 13.$$

is another solution.