Math 6 – Number Theory WS #2

Practice problems

1. Suppose the integer d_1 divides a and the integer d_2 divides b. Must the product $d_1 d_2$ divide ab? If so, why?

2. Use Euclid's algorithm to find the greatest common divisor of 301 and 774; express the gcd as a linear combination of 301 and 774.

Homework

1. Use Euclid's algorithm to find the greatest common divisor of 2231 and 5037. Show your steps!

2. Express the greatest common divisor of 2231 and 5037 as a linear combination of 2231 and 5037. That is, calling the greatest common divisor d, find integers x and y with
$$2231x + 5037y = d.$$

3. For each integer m with $2 \le m \le 20$, compute $(m-1)!$ in $\mathbf{Z}_m$. (For example, $(5-1)! = 24$ in $\mathbf{Z}_5$, which we might notice can also be written as -1.) What patterns do you notice?

Suppose someone asks you to find 2^{100} in $\mathbf{Z}_{137}$? How could you do this without having to compute the entire sequence $2, 2^2, 2^3, \ldots$ up to its hundredth term? Here is one strategy. We compute

$$\begin{array}{ll} 2^0 = 1 & 2^8 = 16^2 = 256 = -18 \\ 2^1 = 2 & 2^{16} = (-18)^2 = 324 = 50 \\ 2^2 = 4 & 2^{32} = 50^2 = 2500 = 34, \\ 2^4 = 16 & 2^{64} = 34^2 = 1156 = 60 \end{array}$$

and then notice that $100 = 64 + 32 + 4$. So in $\mathbf{Z}_{137}$,

$$2^{100} = 2^{64+32+4} = 2^{64} \cdot 2^{32} \cdot 2^4 = 60 \cdot 34 \cdot 16 = 2040 \cdot 16 = -15 \cdot 16 = -240 = 34.$$

4. Using the idea outlined above, compute 3^{50} in $\mathbf{Z}_{97}$. Show your work.

5. The *multiplicative order* of an element a in $\mathbf{Z}_m$ is defined as the smallest exponent $n \ge 1$ for which $a^n = 1$ in $\mathbf{Z}_m$.

   For example, the order of 2 in $\mathbf{Z}_5$ is 4, because in the sequence $2^0 = 1, 2^1, 2^2, 2^3, \ldots$, the first term equal to 1 in $\mathbf{Z}_5$ is 2^4. As another example, 4 has order 2 in $\mathbf{Z}_5$, because $4^0 = 1, 4^1 = 4 = -1$ and $4^2 = (-1)^2 = 1$.

   Pick 5 prime numbers p and record, for each of them, the orders of all the elements of $\mathbf{Z}_p$. Do you notice anything about these numbers in relation to $p-1$? Here is an example for $p = 13$:

	0	1	2	3	4	5	6	7	8	9	10	11	12
order in $\mathbf{Z}_{13}$	$\times$	1	12	3	6	4	12	12	4	3	6	12	2