Last name _____

First name _____

LARSON—MATH 305—CLASSROOM WORKSHEET 25
Sage LAB!—Chinese Remainder Theorem, Extended GCD, Inverses, Powers, Primitive Roots

Organizational Notes

1. A Zoom recording link and class notes will be sent out after each Zoom class.
2. Remember to send your answers to the classroom worksheets, and pdfs of your Lab work. Title your email with enough to help me record your "participation".

Logging into Sage/CoCalc

1. Start the Chrome browser.
2. Go to `http://cocalc.com` and sign in.
3. You should see an existing Project for our class. Click on that.
4. Click "New", call it **c25**, then click "Sage Worksheet".
5. For each problem number, label it in the Sage cell where the work is. So for Problem 1, the first line of the cell should be `#Problem 1`.
6. When you are finished with the worksheet, click "make pdf", email me the pdf (at `clarson@vcu.edu`, with a header that says **Math 305 c25 worksheet attached**).

Chinese Remainder Theorem

1. Find an integer x so that:

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$

   This can be done with the built-in `crt` command. Run: `crt(2,3,3,5)`. Check.

2. Does the following sytem have a solution? If so find it:

$$x \equiv 5 \pmod 7$$
$$x \equiv 3 \pmod{11}$$

Extended GCD

Given integers a, b with $\gcd(a,b) = g$, there are integers x and y such that $g = ax+by$. The *extended GCD algorithm* follows the steps of the GCD algorithm while maintaining enough extra information to construct x and y. Its built-in to Sage.

3. Find the gcd g of 14 and 5. Then use `xgcd(14,5)` to x and y such that $g = 14x+5y$. Check.

4. Find the gcd g of 12 and 8. Then find x and y such that $g = 14x + 5y$. Check.

Inverses

5. To solve the congruence $14x \equiv 1 \pmod 5$ we need to find the multiplicative inverse of $14 \pmod 5$. How can we find that?

   One way is with the built-in `solve_mod` command. Run: `solve_mod([14*x==1],5)`. Check.

6. `solve_mod` also works for quadratic congruences. To solve, the congruence $3x^2+11x+7 \equiv 0 \pmod 5$, run: `solve_mod([3*xˆ2+11*x+7==0],5)`.

Powers

7. We found $3^{147} \pmod 5$ by writing 147 in binary, and finding successive powers of 3 (mod 5). A fast algorithm is built-in to Sage. Run: `power_mod(3,147,5)`.

Primitive Roots

Consider $\mathbb{Z}/n\mathbb{Z}$. There are $\phi(n)$ units. We proved that each of these units has a *multiplicative order* (often just *order*). Recall the order of a unit a is the smallest exponent x such that $a^x \equiv 1 \pmod n$. We will prove that there is a unit a with order $\phi(n)$ (and explore the implications). Such a unit is called a *primitive root*.

8. Find a primitive root in $\mathbb{Z}/3\mathbb{Z}$ by hand. Now run: `primitive_root(3)`.

9. Find a primitive root in $\mathbb{Z}/5\mathbb{Z}$ by hand. Now run: `primitive_root(5)`.

10. Find a primitive root in $\mathbb{Z}/6\mathbb{Z}$ by hand. Now run: `primitive_root(6)`.

11. How could we write an algorithm to find primitive roots?

Extras

12. If p and $p+2$ are both prime, they are called *twin primes*. Find the first several pairs of twin primes.