Last name _____

First name _____

LARSON—MATH 305—SAGE WORKSHEET 06
More Number Theory in Sage.

1. Log in to your Sage Cloud account.
   (a) Start Firefox or Chrome browser.
   (b) Go to `http://cloud.sagemath.com`
   (c) Click "Sign In".
   (d) Click project **Math 305**.
   (e) Click "New", call it **s06**, then click "Sage Worksheet".

2. One of the formulas we proved involved the sum over all the divisors of a number n. How many summand will there be? To find the number of divisors of 12, evaluate: `number_of_divisors(12)`. What are these divisors?

3. Find out how many divisors 1024 has.

4. Find out how many divisors 1,000,000 has.

5. To find out the divisors of 12 that are prime, evaluate: `prime_divisors(12)`.

6. Find the prime divisors of 1024.

7. Find the prime divisors of 1,000,000.

8. The notion of *squarefree integers* played a role in 2 clever proofs of Erdős we discussed. Evaluate: list(squarefree_divisors(12)) to find all of the squarefree divisors of 12.

9. Find all of the squarefree divisors of 100.

10. Find all of the squarefree divisors of 1,000,000. Explain why there are so few.

11. To do **modular arithmetic** in Sage, we first need to tell Sage which number class we are talking about (The numbers $\pmod{10}$, for instance, are different than the numbers $\pmod{20}$: in the first case $2 \cdot 5 \equiv 0$, but not in the second). Find, by hand, $2 \cdot 5 \pmod{10}$.

12. to do this in Sage. We will give the numbers $\pmod{10}$ the name R. Then we'll let a be the number 5 in this collection. Then we'll multiply by 2. Evaluate:

```
R = Integers(10)
a = R(5)
2*a
```

13. Repeat, using $a = 7$. What do you get?

14. Now evaluate: `a**2`. What do you get?

15. Now we want to imitate these ideas to find $51^{2006} \pmod{97}$. What commands will you write? What do you get?

    Fermat's Little Theorem says, if p is prime, then $a^p \equiv a \pmod{p}$. So this is a *necessary condition* for the primality of p. If we check this formula for a randomly chosen a and we don't get a true statement then p is **not** prime. If it is true then it is more **probable** that p is prime. This is the idea behind **pseudoprimality tests**. A test developed from Fermat's Theorem is called the Fermat Primality Test. The truth of congruences can be checked *much faster* than primality itself.

16. Pretend that you don't know if 221 is prime or not, and that $a = 38$ was chosen randomly. Evaluate $38^{221} \pmod{221}$. What do you get? Is the result evidence that 221 is prime?

17. Now pretend that $a = 24$ was chosen randomly. Evaluate 24^{221}. What do you get? Is the result evidence that 221 is prime?

18. Look up the definition of **quadratic residue**. Explain why 4 is a quadratic residue of 5.

19. Evaluate: `quadratic_residues(5)` to find all the quadratic residues of 5.

20. Find all of the quadratic residues of 20.