Math 406 Final Spring 2020

---

1. Given $A = 6259162$ and $B = 206346$. [15 pts]

   (a) Find the prime factorizations of A and B and use them to find $\gcd(A, B)$.

   (b) Find $\gcd(A, B)$ using the Euclidean Algorithm.

2. Use the Chinese Remainder Theorem to find the smallest and second smallest nonnegative solutions to the system: [15 pts]

$$
\begin{aligned}
x &\equiv 2 \bmod 5 \\
x &\equiv 5 \bmod 8 \\
x &\equiv 15 \bmod 17
\end{aligned}
$$

3. For each of $n = 19, 309, 5672, 37699$ find the exact value p_n of the n^{th} prime (however you want) and then approximate value a_n of the n^{th} prime (using the Prime Number Theorem Corollary). Calculate the percentage error [10 pts]

$$\frac{100\,|p_n - a_n|}{p_n}$$

   for each.

4. Find all incongruent solutions mod 124 to the linear system: [10 pts]

$$52x \equiv 4 \bmod 124$$

5. Find all primitive roots for $n = 13$ as follows: First find the smallest positive primitive root. Then use the Theorem from class which yields all the remaining ones. Final answers should be least nonnegative residues. [15 pts]

6. It's a fact that $r = 6$ is a primitive root mod 11. [15 pts]

   (a) Use this to construct a table of indices for this primitive root.

   (b) Use the table of indices to solve the equation: $x^8 \equiv 5 \bmod 11$. Your answer(s) should be mod 11.

   (c) Use the table of indices to solve the equation: $3^x \equiv 5 \bmod 11$. Your answer(s) should be mod 10.

7. Calculate the following Jacobi symbols: [15 pts]

   (a) $\left(\frac{1141}{667}\right)$

   (b) $\left(\frac{1141}{51127}\right)$

8. Suppose you intercept the following ciphertext from Alice to Bob: [15 pts]

```
2982 2237 3239 11364 8541 7043
```

You know that Bob's public key is $(e, n) = (1655, 11639)$. Bob thinks this is secure because he doesn't believe that his n can be factored easily. Factor $n = 11639$, find $\phi(n)$, find d and then decrypt the message. Be clear about the steps you take.

9. Determine if each of the following sets is well-ordered. If a set is not well-ordered give evidence. If a set is well-ordered no evidence is required. [15 pts]

   (a) $\{0\} \cup \left\{ \frac{n+4}{n} \,\middle|\, n \in \mathbb{Z}^+ \right\}$

   (b) $2\mathbb{Z}$

   (c) $\left\{ \lfloor \sqrt{n} \rfloor \,\middle|\, n \in \mathbb{Z}^+ \right\}$

10. Suppose $p \geq 11$ is an unknown prime. Find all solutions to $x^2 + 8 \equiv 6x \bmod p$. Note that your solutions will be mod p. [15 pts]

11. Consider the inequality: [15 pts]

$$3^n < n!$$

   (a) Find the smallest positive integer n_0 for which this is true. Do this however you wish.

   (b) Prove by induction that $3^n < n!$ for all $n \geq n_0$.

12. Suppose p is an odd prime such that there is some a so that a is a quadratic residue of p but $2a$ is a quadratic non-residue of p. Prove that $p \equiv \pm 3 \bmod 8$. [15 pts]

13. Prove that for $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$ that if $a^n \mid b^n$ then $a \mid b$. [15 pts]

14. Prove that if $a, b, c \in \mathbb{Z}$ with $\gcd(a, b) = 1$ and $c \big| (a + b)$ then $\gcd(c, a) = \gcd(c, b) = 1$. [15 pts]