Name:

Math 424: Exam 5

1. (15 pts) Compute $\varphi(735)$.

Solution: Factoring yields $735 = 3 \cdot 5 \cdot 7^2$. Thus

$$\begin{aligned}\varphi(735) &= 735\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)\\ &= 735 \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7}\\ &= 336.\end{aligned}$$

2. (15 pts) Find the remainder when 13^{122} is divided by 225.

Solution: We have $225 = 3^2 \cdot 5^2$, so

$$\varphi(225) = 225 \cdot \frac{2}{3}\frac{4}{5} = 120.$$

As $122 \equiv 2 \pmod{120}$, $13^{122} \equiv 13^2 \pmod{120} = 169$.

3. (15 pts) Given the RSA public key $(n, e) = (551, 5)$, find the private key d.

Solution: We have $551 = 19 \cdot 29$, so $\varphi(551) = 551 \cdot \frac{18}{19} \cdot \frac{28}{29} = 504$. Using the Extended Euclidean algorithm with 504 and 5 yields the modular inverse of 5 mod 504. But there's an easier method: $505 \equiv 1 \pmod{504}$, and also $505 = 5 \cdot 101$. Therefore $101 \equiv 5^{-1} \pmod{504}$. Thus $d = 101$.

4. (15 pts) In RSA, the value of e can never be 100. Explain why not. (The reason is *mathematical*.)

Solution: As $\varphi(n) = (p-1)(q-1)$ and p, q are odd, $\varphi(n)$ is even. Since $2 \mid 100$, with $e = 100$ we'd have $\gcd(e, \varphi(n)) \geq 2$. But we need $\gcd(e, \varphi(n)) = 1$. So $e = 100$ won't work.