BBM 205 - Discrete Structures: Quiz 5 - Solutions
Date: 13.11.2018

Name:
Student ID:

Show all your work to receive full credit.

1. (5 points) What is the remainder of 63^{9601} divided by 220?

> **Solution:** Note that $gcd(63, 220) = gcd(9\cdot 7, 2^2\cdot 5\cdot 11) = 1$. Thus, by Euler's theorem,
>
> $$63^{\Phi(220)} \equiv 1 \pmod{220}.$$
>
> We can calculate $\Phi(220)$ by using the distinct prime divisors of 220 as $p_1 = 2$, $p_2 = 5$, $p_3 = 11$.
>
> $$\Phi(220) = 220\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right) = 220\frac{1}{2}\cdot\frac{4}{5}\cdot\frac{10}{11} = 80.$$
>
> So, $63^{80} \equiv 1 \pmod{220}$. Therefore,
>
> $$\begin{aligned} 63^{9601} \pmod{220} \equiv 63^1 \cdot (63^{80})^{120} \pmod{220} &\equiv \\ \equiv 63^1 \cdot 1^{120} \pmod{220} \equiv 63 \pmod{220}.& \end{aligned}$$

2. (5 points) Simplify the following expression $3^{33} \pmod{11}$ using Fermat's Little Theorem.

> **Solution:**
>
> $$3^{33} \pmod{11} \equiv 3^3 \cdot (3^{10})^3 \pmod{11} \equiv 27 \cdot 1^3 \pmod{11} \equiv 5 \pmod{11}.$$

3. Bob would like to receive encrypted messages from Alice via RSA.

   (a) (2 points) Bob chooses $p = 7$ and $q = 11$. His public key is (N, e). What is N?

   Solution: $N = pq = 77$.

   (b) (2 points) What number is e relatively prime to?

   Solution: e must be relatively prime to $(p-1)(q-1) = 60$.

   (c) (2 points) e need not be prime itself, but what is the smallest prime number e can be? Use this value for e in all subsequent computations.

   Solution: We cannot take $e = 2, 3, 5$, so we take $e = 7$.

   (d) (2 points) What is $\gcd(e, (p-1)(q-1))$?

   Solution: By the RSA method's definition, $gcd(e, (p-1)(q-1)) = 1$.

   (e) (2 points) What is the decryption exponent d? Do not calculate d, only describe what condition d should satisfy.

   Solution: The decryption exponent is $d = e^{-1} \pmod{60}$