MIDTERM 2 REVIEW

COMPUTER SCIENCE MENTORS 70

October 23, 2016

1 FLT and RSA

1. **Becoming Alice**
Alice wants to send Bob a message $m = 5$ using his public key $(n = 26, e = 11)$. What ciphertext $E(m)$ will Alice send? How will Bob decode it?

Solution:

$$\begin{aligned}
5^1 &\equiv 5 \mod 26 \\
5^2 &\equiv 25 \mod 26 \\
&\equiv -1 \mod 26 \\
5^4 &\equiv (-1)^2 \mod 26 \\
&\equiv 1 \mod 26 \\
5^8 &\equiv 1 \mod 26 \\
5^{11} &\equiv 5^8 * 5^2 * 5^1 \mod 26 \\
&\equiv 1 * -1 * 5 \mod 26 \\
&\equiv -5 \mod 26 \\
&\equiv 21 \mod 26
\end{aligned} \tag{1}$$

So our encoded message is $C = 21$. To find d, we need to factor N into its two prime factors, P and Q which are 2 and 13, and then find: $e-1 \mod (p-1)(q-1)$, so find $11 - 1 \mod 12; d = 11$ $C^d \mod N = 21^{11} \mod 26 = 5$