Your Name Goes Here

Math 25

Homework 6

1. **An encryption problem**

Background: Let's use a 27-letter alphabet with $A \leftrightarrow 0$, $B \leftrightarrow 1$, $\ldots$, $Z \leftrightarrow 25$, space $\leftrightarrow 26$. We shall convert between alphabetic and numeric plaintext messages by a common scheme: encoding as a base 27 number with a certain block size, in our case 5. We do this as follows: Suppose we want to convert the message 'Groups are fun'.

First we break up our plaintext message into blocks of length 5, padding the last block if necessary: '`Group`' '`s␣are`' '`␣funX`'. Note we will not distinguish between upper and lower case, but this would easily be done by expanding the size of our alphabet.

'`Group`' $\mapsto 06, 17, 14, 20, 15$; '`s␣are`' $\mapsto 18, 26, 00, 17, 04$; '`␣funX`' $\mapsto 26, 05, 20, 13, 23$, where the numbers represent the base-27 digits. We now encode these as base 27 numbers:

$$\begin{aligned}
\texttt{Group} &\mapsto 06, 17, 14, 20, 15 \\
&\mapsto 27^4(06) + 27^3(17) + 27^2(14) + 27^1(20) + 27^0(15) = 3534018 \\
`\texttt{s}\sqcup\texttt{are}' &\mapsto 18, 26, 00, 17, 04 \\
&\mapsto 27^4(18) + 27^3(26) + 27^2(00) + 27^1(17) + 27^0(15) = 10078170 \\
\sqcup\texttt{funX} &\mapsto 26, 05, 20, 13, 23 \\
&\mapsto 27^4(26) + 27^3(05) + 27^2(20) + 27^1(13) + 27^0(23) = 13930835
\end{aligned}$$

To proceed, we note that all the plaintext messages P will satisfy $0 \leq P < 27^5 = 14,348,907$, so when choosing primes p, q for our RSA modulus $n = pq$, we must make sure $n \geq 27^5$.

The exercise. Suppose we choose primes p and q, so that $n = pq = 59753237$. With the knowledge of those primes, we compute $\phi(n) = (p-1)(q-1) = 59737740$, and choose the common encryption exponent $e = 2^{16} + 1 = 65537$ (the last known Fermat prime).

(a) Find the primes p and q using the idea from your notes. That is, do not just factor n (try to think that n could have been a 600 digit number instead). Finding p and q is not necessary to break the code, but reinforces that knowing $\phi(n)$ is equivalent to factoring n.

(b) Find the decryption exponent.

(c) Using the base 27 encoding scheme as above, decrypt the message consisting of two blocks of numerical ciphertext,
i.e., given as $C = P^e \pmod{n}$: 10881312 41465338.

2. Suppose that $m, n > 1$ are coprime integers. Prove that

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}.$$

3. Show that 5 is a primitive root modulo 40487, but not one modulo 40487^5. Find a primitive root mod 40487^5, and prove your result. Feel free to use a computational tool like Sage to help with the computations.

4. Let $n > 2$ be an integer, and $a \in \mathbb{Z}$.

   (a) Suppose that $a^k \equiv a^\ell \equiv 1 \pmod{n}$. Show that $a^d \equiv 1 \pmod{n}$, where $d = \gcd(k, \ell)$.

   (b) Suppose that $a^{n-1} \equiv 1 \pmod{n}$ and $a^{(n-1)/q} \not\equiv 1 \pmod{n}$ for all primes $q \mid n-1$. Show that n must be prime.

   Below is a table which gives each reduced residue mod 23 in terms of the primitive root 5.

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
5^k	5	2	10	4	20	8	17	16	11	9	22	18	21	13	19	3	15	6	7	12	14	1

5. Use the information above to find all solutions to $3x^{10} \equiv 1 \pmod{23}$.

6. Use the information above to find all solutions to $13^x \equiv 5 \pmod{23}$.