MME 529 HW 7

1. Use Fermat's Little Theorem to show 297 is not prime.

FLT states that if p is prime, then $a^p \equiv a \bmod p$ for any $a \in \mathbb{Z}$. Since $2^{297} \equiv 161 \bmod 297 \not\equiv 2 \bmod 297$, conclude that 297 must be composite.

2. a) Simplify $5^{5281} \bmod 37$.

By FLT, $5^{36} \equiv 1 \bmod 37$. Since $5281 = 146 \cdot 36 + 25$,

$5^{5281} \bmod 37 \equiv (5^{36})^{146} 5^{25} \bmod 37 \equiv 1^{146} 5^{25} \bmod 37 \equiv 5^{25} \bmod 37$

Since $5^3 \equiv 14 \bmod 37$, $5^{24} \equiv 14^8 \bmod 37 \equiv (14^2)^4 \bmod 37$
$\equiv 11^4 \bmod 37 \equiv 10^2 \bmod 37 \equiv 26 \bmod 37$.

$5^{25} \bmod 37 \equiv 5^{24} \cdot 5 \bmod 37 \equiv 26 \cdot 5 \bmod 37 \equiv 130 \bmod 37 \equiv \underline{19 \bmod 37}$.

3. Develop a 2x2 matrix that could encrypt/decrypt a pair of numbers or symbols mod 31.

Let $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ be the encryption matrix. Then

$A^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 30 \\ 0 & 1 \end{pmatrix} \bmod 31$. To encrypt "PI", encode the message as $d = (16, 9)^T$. The encrypted vector e is

$$(Ad) \bmod 31 = \begin{pmatrix} 25 \\ 9 \end{pmatrix} \bmod 31, \quad e = \begin{pmatrix} 25 \\ 9 \end{pmatrix}$$

To decrypt, we should be able to recover $d = \begin{pmatrix} 1 & 30 \\ 0 & 1 \end{pmatrix} e \bmod 31$.

$$\begin{pmatrix} 1 & 30 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 25 \\ 9 \end{pmatrix} = \begin{pmatrix} 295 \\ 9 \end{pmatrix} \equiv \begin{pmatrix} 16 \\ 9 \end{pmatrix} \bmod 31 = d.$$

5. Consider the RSA Theorem. Where does the proof break down if P, q are not prime?

We used FLT to get $(B^{P-1})^{q-1} \equiv 1 \bmod P$, $(B^{q-1})^{P-1} \equiv 1 \bmod q$. These congruences do not hold generally if P, q are composite.

6. Pick 2 primes and develop an encrypt/decrypt scheme.

$p = 51$, $q = 63$, $n = pq = 3233$, $\lambda(n) = \text{lcm}(p-1, q-1) = 780$

$e = 17$, $d = 413$, $ed \equiv 1 \bmod \lambda(n)$

$(e, n) = (17, 3233)$ public $(d, n) = (413, 3233)$ private

To encrypt $D = 206$, we calculate

$$E = D^e \bmod n = 206^{17} \bmod 3233 = 24$$

$E = 24$ is the encrypted version of $D = 206$.
To recover D from E using the private key, compute

$$E^d \bmod n = 24^{413} \bmod 3233 = 206 = D \checkmark$$

7. Suppose that $a^k \equiv 1 \bmod p$ for some $a \in \mathbb{Z}_p$, p prime, and $0 < k < p-1$. What relation must k have to p?

We must have $k \mid p-1$. Assume k is the smallest possible integer s.t. $0 < k < p-1$ and $a^k \equiv 1 \bmod p$. By the E.A., $\exists\, q, r$ s.t. $p-1 = qk + r$. Then, by FLT,

$$1 \equiv a^{p-1} \bmod p \equiv (a^k)^q a^r \bmod p \equiv a^r \bmod p.$$

But since $0 \leq r < k$ and k is the smallest positive integer s.t. $a^k \equiv 1 \bmod p$, we must have $r = 0$ to satisfy $1 \equiv a^r \bmod p$. Therefore, $p-1 = qk$, showing that $k \mid p-1$.

8. In $\mathbb{Z}_{13}$, what is $\log_6 7$?

We must find $6^y \equiv 7 \bmod 13$. Testing increasing powers y gives: $6^7 \equiv 7 \bmod 13$. $\therefore$ $\log_6 7 = 7$ in $\mathbb{Z}_{13}$.