# Quiz #1

**MATH 481/581 — Cryptography**
**Wednesday, Jan 25**

***Please print your name:***

---

**Problem 1.** Express 42 in base 5.

**Solution.** $42 = 8 \cdot 5 + \boxed{2}$, $8 = 1 \cdot 5 + \boxed{3}$, $\boxed{1}$

Hence, $42 = (132)_5$. □

**Problem 2.** Evaluate $80^{609} \pmod{77}$. [Simplify before binary exponentiation!]

**Solution.** Obviously, $80^{609} \equiv 3^{609} \pmod{77}$. We note that $\gcd(3, 77) = 1$, so that we may apply Euler's theorem.

Since $\phi(77) = \phi(7 \cdot 11) = \phi(7)\phi(11) = 60$, we conclude that $3^{609} \equiv 3^9 \pmod{77}$.

Using binary exponentiation, $3^2 = 9$, $3^4 = 9^2 \equiv 4$, $3^8 \equiv 16$. Hence, $3^9 = 3 \cdot 3^8 \equiv 3 \cdot 16 = 48 \pmod{77}$.

In summary, $80^{609} \equiv 48 \pmod{77}$.

□

**Problem 3.** Find the modular inverse of 12 modulo 101.

**Solution.** We determine $12^{-1} \pmod{101}$ using the extended Euclidean algorithm:

$$\begin{array}{lll} \gcd(12, 101) & \boxed{101} = 8 \cdot \boxed{12} + 5 & \text{or: } \boxed{A}\ \ 5 = \boxed{101} - 8 \cdot \boxed{12} \\ = \gcd(5, 12) & \boxed{12} = 2 \cdot \boxed{5} + 2 & \boxed{B}\ \ 2 = \boxed{12} - 2 \cdot \boxed{5} \\ = \gcd(2, 5) & \boxed{5} = 2 \cdot \boxed{2} + 1 & \boxed{C}\ \ 1 = \boxed{5} - 2 \cdot \boxed{2} \\ = 1 & & \end{array}$$

Backtracking through this, we find that **Bézout's identity** takes the form

$$1 \underset{\boxed{C}}{=} \boxed{5} - 2 \cdot \boxed{2} \underset{\boxed{B}}{=} -2 \cdot \boxed{12} + 5 \cdot \boxed{5} \underset{\boxed{A}}{=} 5 \cdot \boxed{101} - 42 \cdot \boxed{12}$$

Hence, $12^{-1} \equiv -42 \pmod{101}$. (Equivalently, $12^{-1} \equiv 59 \pmod{101}$.)

□

Armin Straub
straub@southalabama.edu