Quiz #1

MATH 311 — Intro to Number Theory
Thursday, Sep 26

Please print your name:

Problem 1. Using the Euclidean algorithm, find the modular inverse of 17 modulo 23.

Solution. We apply the extended Euclidean algorithm:

$$\begin{array}{lll} \gcd(17,23) & \boxed{23} = 1\cdot\boxed{17} + 6 & \text{or: } \boxed{A} \quad 6 = 1\cdot\boxed{23} - 1\cdot\boxed{17} \\ = \gcd(6,17) & \boxed{17} = 3\cdot\boxed{6} - 1 & \quad\;\;\; \boxed{B} \quad 1 = -1\cdot\boxed{17} + 3\cdot\boxed{6} \\ = 1 & & \end{array}$$

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

$$1 \underset{\boxed{B}}{=} -1\cdot\boxed{17} + 3\cdot\boxed{6} \underset{\boxed{A}}{=} 3\cdot\boxed{23} - 4\cdot\boxed{17}$$

In summary, we have $1 = -4\cdot 17 + 3\cdot 23$ (that is, $d=1$, $x=-4$, $y=3$). Hence, $17^{-1} \equiv -4 \pmod{23}$. ☐

Problem 2. Determine $40^{1612} \pmod{17}$. Carefully show all steps!

Solution. First, we simplify base and exponent $40^{1612} \equiv 6^{1612} \equiv 6^{12} \pmod{17}$. For the second congruence, we used Fermat's little theorem and $1612 \equiv 12 \pmod{16}$.

We now use binary exponentiation: $6^2 \equiv 2 \pmod{17}$, $6^4 \equiv 2^2 = 4 \pmod{17}$, $6^8 \equiv 4^2 \equiv -1 \pmod{17}$

It follows that $6^{12} = 6^8 \cdot 6^4 \equiv -1\cdot 4 \equiv -4 \pmod{17}$.

In conclusion, $40^{1612} \equiv -4 \pmod{17}$. ☐

Problem 3. The number 55 in base 5 is $\boxed{}$.

Solution. $55 = 2\cdot 5^2 + 5 = (210)_5$ ☐

Armin Straub
straub@southalabama.edu