Ma2201/CS2022 — Discrete Mathematics — D Term, MMXVI

Quiz 0110

Print Name: ____________________

Sign: ____________________

1. (**3 points**) Find the multiplicative inverse of 10 in $\mathbb{Z}_{23}$.

♣ *Euclidean Algorithm:*

$$23 = 2 \cdot 10 + 3$$
$$10 = 3 \cdot 3 + 1$$

Adding -3 *times the first with the second gives*

$$(-3)(23) + (7)(10) = 1$$

so 7 *is the multiplicative inverse.*

2. (**3 points**) In an RSA scheme the two primes are $p = 17$ and $q = 11$.
Give three odd two digits numbers which would *not* work as encoding or decoding keys.

♣ *The encoding keys must have multiplicative inverses modulo* $(p-1)(q-1) = (16)(10) = 2^5 5$. *So encoding keys must be coprime to* 160, *that is to* 2 *and* 5. *So the only two digit odd numbers which do not work are* 15, 25, 35, 45, *etc.*

3. (**4 points**) Compute 2^{2016} modulo 101.

♣ *According to Fermat's Little Theorem* $2^{100} \equiv 1 \bmod 101$, *so* $2^{2016} = 2^{2000} 2^{16} = (2^{100})^{20} 2^{16} \equiv 2^{16} \bmod 101$. *From there it is easy. Most people know*

$2, 4, 8, 16, 32, 64, 128, 256, 512, 1024$, *so*

$2^{10} \equiv 1024 \equiv 14 \bmod 101$.

$2^{11} \equiv 28 \bmod 101$.

$2^{12} \equiv 56 \bmod 101$.

$2^{13} \equiv 112 \equiv 11 \bmod 101$.

$2^{14} \equiv 22 \bmod 101$.

$2^{15} \equiv 44 \bmod 101$.

$2^{16} \equiv 88 \bmod 101$.