tags: ***MATA02-2022***

MATA02-2022: Quiz 4 Practice [20pts total]

During tutorials week 10: March 21-25
Write your name and Student Number on every single page of work, or else you will not get credit

1. [5pts]

Solve the following division problem in modular arithmetic, or say that there is no unique answer. If there is no unique answer, explain why.

$$12/23 \mod 79$$

First find $\frac{1}{23}$

$79 = 23 \cdot 3 + 10$
$23 = 10 \cdot 2 + 3$
$10 = 3 \cdot 3 + 1$
$1 = 3 \cdot 1$

Thus
$1 = 10 - 3 \cdot 3$
$1 = 10 - (23 - 10 \cdot 2) \cdot 3$
$1 = 10 \cdot 7 - 23 \cdot 3$
$1 = (79 - 23 \cdot 3) \cdot 7 - 23 \cdot 3$
$1 = 79 \cdot 7 - 23 \cdot 24$

Taking mod of everything
$1 \equiv -23 \cdot 24 \mod 79$
$1 \equiv 23 \cdot (-24) \mod 79$
$1 \equiv 23 \cdot 55 \mod 79$

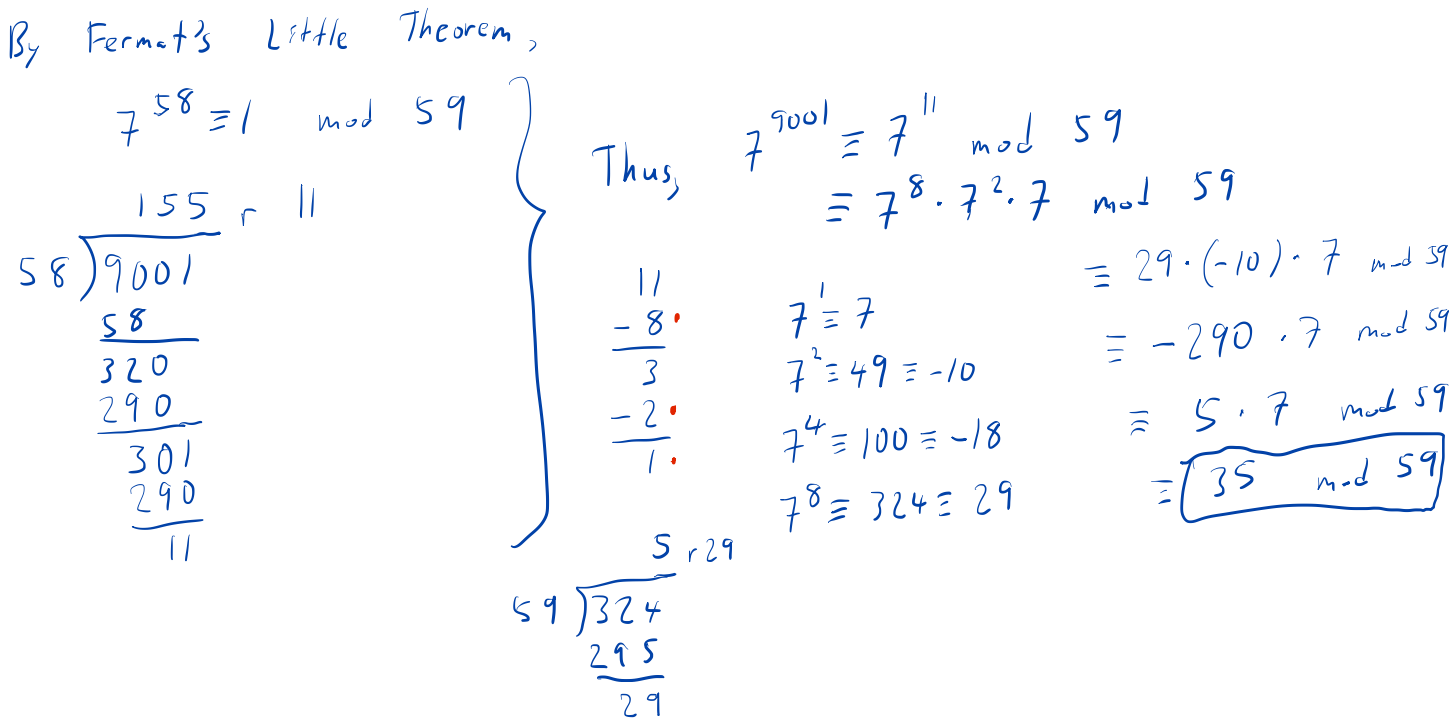
$\frac{1}{23} \equiv 55 \mod 79$

Multiplying
$\frac{12}{23} \equiv 12 \cdot 55 \equiv 660 \mod 79$
$\equiv 28 \mod 79$

2. [5pts]

Solve the following power problem in modular arithmetic.

$$7^{9001} \mod 59$$



3. [10pts]

Below is an attempted proof. Say whether each line of the proof is correct, assuming all previous lines are correct. Please justify your assertion of whether it is right or wrong for each line.
Note that notationally, I will use "$\equiv$" sometimes without specifying the modulus, but that is not to be considered an error.

Theorem and proof

I claim that if $n^2 \equiv 1 \mod 3$, then $n \equiv 1 \mod 3$.

1. Suppose for the sake of contradiction that $n \not\equiv 1 \mod 3$.
2. Then $n \equiv 2 \mod 3$.
3. But by the rules of multiplication in modular arithmetic, $n^2 \equiv 2^2 \equiv 4 \equiv 1 \mod 3$.
4. Therefore, to conclude, if $n^2 \equiv 1 \mod 3$, then $n \equiv 1 \mod 3$.

There are two lines wrong in the proof.

Line 1 is the correct setup for a proof by contradiction.

Line 2 is wrong because n could be congruent to either 0 or 2, and we are only checking one case.

Line 3 is correct, because it is just using the rules of arithmetic.

Line 4 is wrong because even if all the previous lines are correct, we setup a proof by contradiction, and never found a contradiction.

Extra space for problem 3