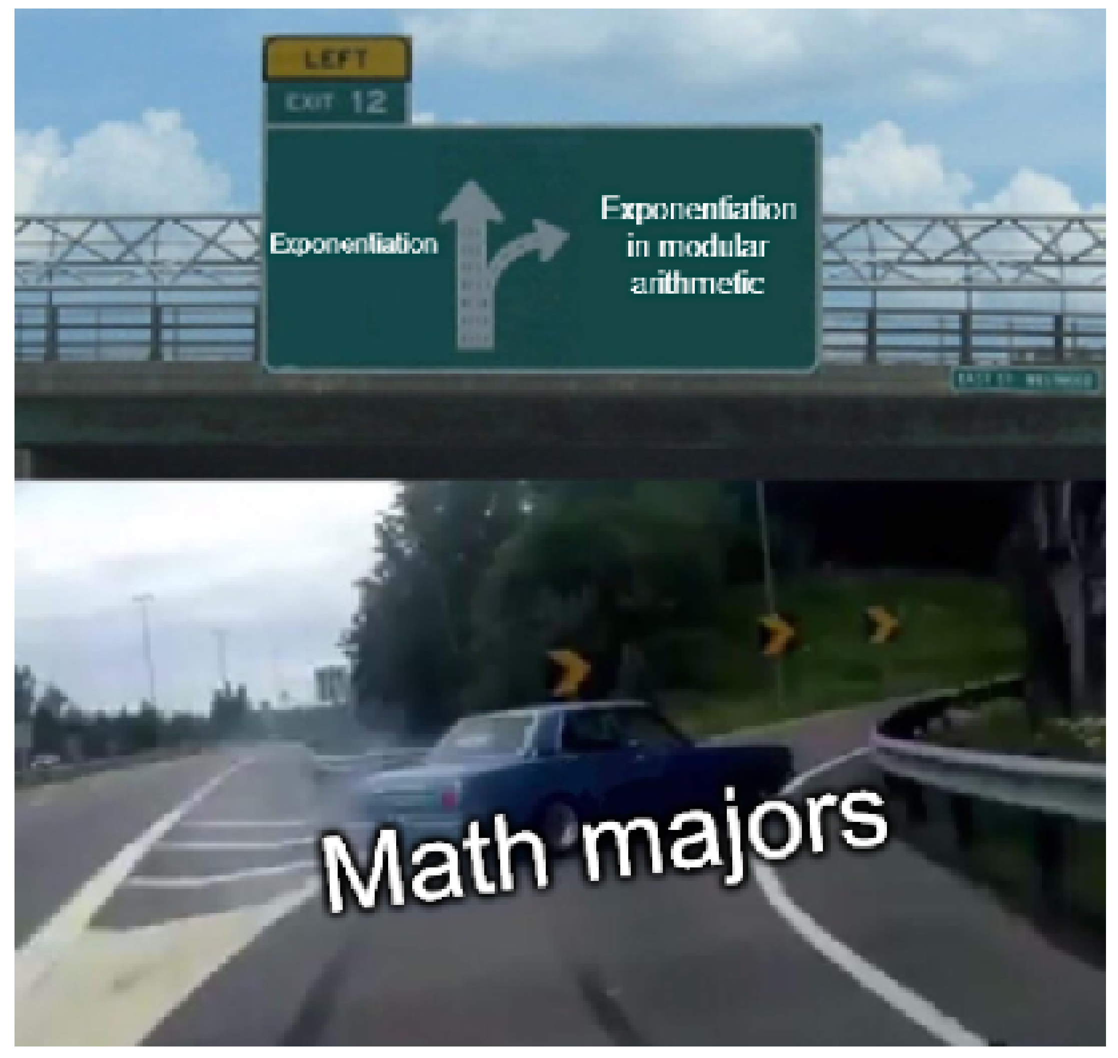


We might not get into modular exponentiation, but it is an important tool in cryptography. It's more fun than real exponentiation (which is not fun by hand).

1 a,b

1. Determine if the following congruences are true (using the definition of congruency, and prefer- ably without a calculator).

a. $430023 \equiv 23 \pmod{43}$

b. $23 \equiv 430023 \pmod{43}$

a. This is true as $430023 = 43*10000 + 23$. So $43|(430023 - 23)$.

b. This is true as $23 - 430023 = -430000 = 43*-10000$. So $43|(23 - 430023)$

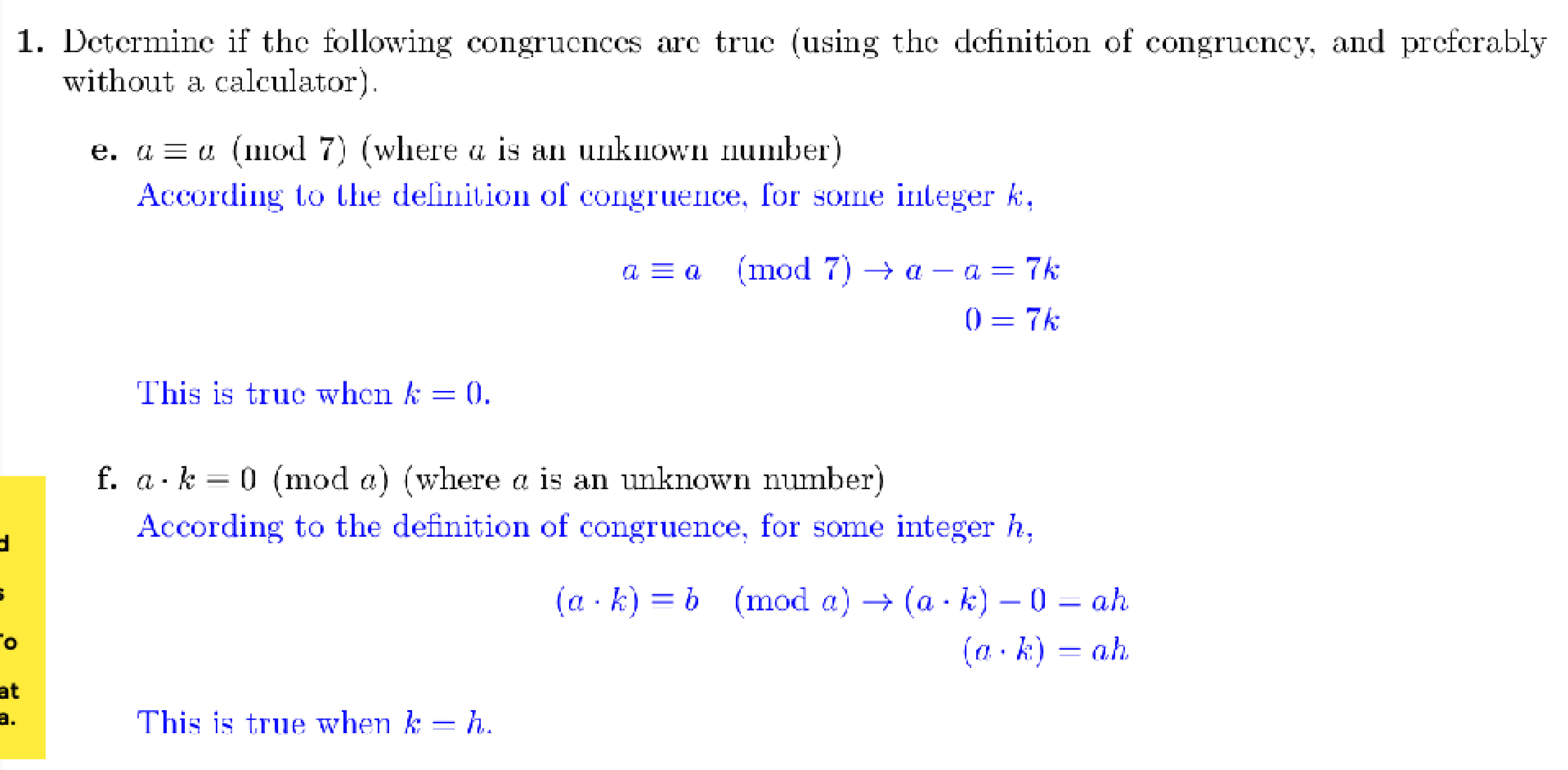
- Miah :)

1 c,d

c: NOT true because the difference between those two numbers will not have a 0 ending and hence is not divisible by 10.

d: TRUE because the difference between those two numbers ends with 5 (positive or negative) and is divisible by 5.

1 e,f



1. Determine if the following congruences are true (using the definition of congruency, and preferably without a calculator).

   e. $a \equiv a \pmod{7}$ (where a is an unknown number)

   According to the definition of congruence, for some integer k,

$$\begin{aligned} a \equiv a \pmod{7} \to a - a &= 7k \\ 0 &= 7k \end{aligned}$$

   This is true when $k = 0$.

   f. $a \cdot k = 0 \pmod{a}$ (where a is an unknown number)

   According to the definition of congruence, for some integer h,

$$\begin{aligned} (a \cdot k) = b \pmod{a} \to (a \cdot k) - 0 &= ah \\ (a \cdot k) &= ah \end{aligned}$$

   This is true when $k = h$.

I'm a bit confused here. I think we need a bit more clarification in terms of what's assumed and what's shown. To show a*k=0 (mod a) we need to show that a*k-0 is divisible by a.

I think you're saying "a*k=0 (mod a) if a*k-0=a*k is divisible by a. This is true because a*k is a*h, where h is an integer, with h=k." Is that what you mean?

2

Divisibility rule by 3: Add the digits. Whatever the remainder of this number is when it's divided by 3 is the remainder of the whole number divided by 3.

The first number: We don't have to add all the digits. We can add little by little, and "throw away" (or is it "casting out"?) any multiple of 3 we get. So first two digits, 1+2 is a multiple of 3. Throw away.

Then comes 3. Throw away. Then 4+5, throw away. Then throw 6 away. Then 7+7+7, throw away. So the remainder is 1. We can say "first number"=1 (mod 3)

Next number: 1+1+1... gone. 2+3+4... gone. Another 1+1+1, gone. So the remainder is 2. So "next number"=2 (mod 3).

3

Say
$a = 7m + 4$
and
$b = 7n + 5$

$a + b = 7m + 4$
$+ 7n + 5$
$= 7(m+n+1) + 2$
$= 7k + 2$

$a - b = 7m + 4 - 7n - 5$
$= 7(m-n) + (-1)$
$= 7(m-n) + (-1+7) - 7$
$= 7(m-n-1) + 6$
$= 7k + 6$

$ab = (7m+4)(7n+5)$
$= 49mn + 35m + 28n$
$+ 20 =$
$7(7mn+5m+4n+2) + 6$
$= 7k + 6$

$a+b$ is 2 mod 7
$a-b$ is 6 mod 7
ab is 6 mod 7

Cian

4

"Simplify the expression 25*34+9*8ˆ12 (mod 7). Justify briefly."

The justifications in question 3 can be generalized to show that for addition, subtraction, and multiplication in modular arithmetic, remainders can be calculated...

... before, during, and after an expression is evaluated.

Thus we can reduce each of the integers (not 12 because it's an exponent) in the expression (mod 7) before evaluating it, and reduce our result (mod 7) if necessary.

Specifically, if a==r_a (mod m) and b==r_b (mod m) then a+b==r_a+r_b (mod m), a-b==r_a-r_b (mod m), and ab==r_a*r_b (mod m). Where "==" denotes congruency.

The expression then becomes 4*6+2*1ˆ12 = 26.

26==5 (mod 7) so 25*34+9*8ˆ12==5 (mod 7)

-Nick

Last page