MAT 1830 Applied W2

Tutorial Sheet #1

Show your working for all questions.

1. Are the following statements true or false? Why?

(a) $14 \equiv 20 \mod 8$
False
$8 \nmid (14 - 20) = -6$

(b) $3 \mid -15$
True
$-15 = 3 \times (-5)$

(c) $-11 \equiv 1 \mod 3$
True
$3 \mid (-11 - 1) = -12$

(d) 9 is prime
$1 \mid 9, 3 \mid 9, 9 \mid 9$
Other divisor than 1 and 9

(e) $1000 \equiv 12544 \mod 5$

(f) $66 \mid 22$
$22 = 0 \times 66 + 22$
$r \neq 0$ so $66 \nmid 22$

2.

(a) Use the Euclidean algorithm to find the greatest common divisor of 1022 and 400.
Solution:

$$\begin{aligned} 1022 &= 2 \times 400 + 222 \\ 400 &= 1 \times 222 + 178 \\ 222 &= 1 \times 178 + 44 \\ 178 &= 4 \times 44 + 2 \\ 44 &= 22 \times 2 + 0 \end{aligned}$$

(b) Find integers a and b such that $\gcd(1022, 400) = a \times 1022 + b \times 400$.
$2 = 23 \times 400 - 9 \times 1022$
$a = -9, b = 23$

(c) Find integers a and b such that $8 = a \times 1022 + b \times 400$ or explain why they don't exist.
$8 = -36 \times 1022 + 92 \times 400$
solving this is equivalent to find z such that

$$400z \equiv 8(\bmod 1022)$$

3.

(a) Let n be an integer. If x is the smallest integer such that $x > 2$ and x divides n, must x be prime? How do you know?

(b) Let y be an integer such that $y \equiv 2 \mod 3$. For what integers z with $0 \leq z \leq 11$ is it possible that $y \equiv z \mod 12$? Explain your answer carefully.

4.

(a) Imagine you are Commissioner Gordon, chief of the Gotham City police. The Joker has set up a bomb which will explode unless a jug containing exactly 4L of water is placed on a scale. Only jugs with capacities of 7L, 21L, and 28L can be used to obtain this amount. Do you send Barbara Noether (Gotham's foremost expert on maths) or Batman (Gotham's foremost expert on punching the Joker and stopping things from blowing up)?
Impossible to get 4L with jugs whose volume is multiple of 7
(b) Look back at 2(b). Is the solution you found the only solution?
Not the only solution.

$$\begin{aligned}\gcd(1022, 400) &= 2 = 23 \times 400 - 9 \times 1022 \\ &= 23 \times 400 - 9 \times 1022 + k \times 400 \times 1022 - k \times 400 \times 1022 \\ &= (23 + 1022k) \times 400 - (9 + 400k) \times 1022, k \in \mathbb{Z}\end{aligned}$$

So there are infinite many solutions.
Moreover, since k is any integer, we can rescale it as what we want. dividing by the gcd of 1022 and 400, we have

$$a = -9 + 200k$$

$$b = 23 + 511k$$

Such equation is named after *Diophantine equation*, it follows that

$$\gcd(a, b) = a \cdot m + b \cdot n$$

The specific solution a_0, b_0 has the following relation with the general solution a, b.

$$a = a_0 + \frac{kn}{\gcd(a, b)}$$

$$b = b_0 + \frac{km}{\gcd(a, b)}$$

Practice Questions

1.

Find integers x and y such that $605x + 210y = 10$.
Refer to problem 2 in the last section

2.

Prove that if x and y are integers such that $x \equiv 2(\bmod 8)$ and $y \equiv 7(\bmod 8)$, then 8 divides $2(x+y)^{13} + y - 1$.
Proof:
Because $x \equiv 2 \bmod 8$, and $y \equiv 7(\bmod 8)$
and

$$a \equiv b(\bmod m), b \equiv c(\bmod m) \implies a \equiv c(\bmod m)$$

We have $(x+y) \equiv 9 \bmod 8$, while obviously $9 \equiv 1(\bmod 8)$.
Therefore, it holds that $(x+y) \equiv 1(\bmod 8)$.
By the property of modular congruence,

$$a \equiv b \bmod m, c \equiv b \bmod m \implies ac \equiv b^2(\bmod m) \quad (1)$$

Using Eq.1 repetitively gives us $(x+y)^{13} \equiv 1(\bmod 8)$
Also by $a \equiv b(\bmod m) \implies ca \equiv cb(\bmod m)$, we have $2(x+y)^{13} \equiv 2(\bmod 8)$
And

$$a \equiv b(\bmod m), c \equiv d(\bmod m) \implies a + c \equiv b + d(\bmod m)$$

if and only if $y \equiv 7 \bmod 8 \implies (y-1) \equiv 6(\bmod 8)$
Again, by Eq.1, $2(x+y)^{13} + y - 1 \equiv 8(\bmod 8)$.
By definition of congruence

$$a \equiv b(\bmod m) \iff a \bmod m = b \bmod m$$

Hence we have

$$[2(x+y)^{13} + y - 1] \bmod 8 = 8 \bmod 8 = 0 \iff [2(x+y)^{13} + y - 1] = 8k, k \in \mathbb{Z}$$

$$[2(x+y)^{13} + y - 1] = 8k, k \in \mathbb{Z} \iff 8 \mid [2(x+y)^{13} + y - 1]$$

Therefore, 8 divides $2(x+y)^{13} + y - 1$. This completes the proof.
Q.E.D.

3.

You're trying to find the gcd of two 21 (decimal) digit numbers on a computer which can do 1000 division-remainder operations every second.

(a) Can you show that if the number “on the left” of a line of the Euclidean algorithm is a, then the number on the left two lines down must be less than $\frac{a}{2}$?

Proof:

For the execution of $\gcd(a, b)$

It follows that

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \end{aligned}$$

the number the left two lines down is exactly r_1, and $r_1 = a \bmod b$

This means that $\forall r_1 \in \mathbb{z}, 1 \leq r_1 < b$.

On the other hand, $\frac{a}{2} \equiv a \div 2 \equiv (a = 2k + r), k \in \mathbb{z}, r \in \{0, 1\}$.

This is exactly the case when b = 2 for some integer $a = 2q_1 + r_1$. This is already the most extreme case that we can use Euclidean algorithm, because when $b = 1$ we can only have $r_1 = 0$, which means $b \mid a$, and also $b \leq \frac{a}{2}$.

If there exists a second row in the process, we must have $r_1 \nmid b, r_2 \neq 0$.

In the same way, we have $r_1 \leq \frac{b}{2}$. Therefore, we have

$$r_1 \leq \frac{b}{2} < b \leq \frac{a}{2} < a$$

Hence, $r_1 < \frac{a}{2}$, and r_1 is exactly the element two line down on the left with respect to a . This completes the proof.

Q.E.D.

(b) If you halve any 21 digit number 70 times, the result will be less than 2 (this is because $\log_2(10^{21}) < 70$). What can you say about how long your computer will take to run the Euclidean algorithm on your numbers?

Solution:

Even in the worst cases where every step, $b = \frac{1}{2}a$, there will be 140 division to be done. That takes $\frac{140}{1000} = 0.14$ second. So, it is confirmed that the operation could be done within at most 0.14 second.

(c) You consider finding prime factorisations of your two numbers instead. About how long would it take your computer to try dividing a 21 digit number by every number up to $\sqrt{n}$?

$$\sqrt{10^{21}} = (10^{21})^{0.5} = 10^{10.5}$$

$$10^{10.5} \div 10^3 = 10^{10.5} \times 10^{-3} = 10^{7.5} > 100,000,00$$

So it could iterate more than ten million second to reach $\sqrt{n}$, this is more than 100 days.

4.

(a) Use the Euclidean algorithm to find the greatest common divisor of 21 and 13, and the greatest common divisor of 34 and 21.

$\gcd(21, 13) = 1$, $\gcd(34, 21) = 1$.
(b) It turns out that 21 and 13 is the smallest pair of numbers for which the Euclidean algorithm requires 6 steps (for every other pair a and b requiring 6 or more steps, $a > 21$ and $b > 13$). Given this, what can you say about 34 and 21?
The smallest pair of numbers for 7 steps to finish Euclidean algorithm.
(c) Can you guess the smallest pair of numbers requiring 8 Euclidean algorithm steps?
$\gcd(55, 34)$
(d) Is there a pattern here? Do the numbers which keep coming up have a name?
They are all in the Fibonacci Sequence.