MAT1830 - Discrete Mathematics for Computer Science
Tutorial Sheet #1

Show your working for all questions.

1. Are the following statements true or false? Why?
   (a) $14 \equiv 20 \pmod 8$
   (b) 3 divides -15
   (c) $-11 \equiv 1 \pmod 3$
   (d) 9 is prime
   (e) $1000 \equiv 12544 \pmod 5$
   (f) 66 divides 22

2. (a) Use the Euclidean algorithm to find the greatest common divisor of 1022 and 400.
   (b) Find integers a and b such that $\gcd(1022, 400) = a \times 1022 + b \times 400$.
   (c) Find integers a and b such that $8 = a \times 1022 + b \times 400$, or explain why they don't exist.

3. (a) Let n be an integer. If x is the smallest integer such that $x \geqslant 2$ and x divides n, must x be prime? How do you know?
   (b) Let y be an integer such that $y \equiv 2 \pmod 3$. For what integers z with $0 \leqslant z \leqslant 11$ is it possible that $y \equiv z \pmod{12}$? 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)? Batman to hit Joker
   (b) Look back at 2(b). Is the solution you found the only solution?

(See over for practice questions.)

Practice Questions

1. Find integers x and y such that $605x + 210y = 10$.

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

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 $\frac{a}{2}$?

   (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?

   (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 n by every number up to $\sqrt{n}$?

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.

   (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 $a \geqslant 21$ and $b \geqslant 13$). Given this, what can you say about 34 and 21?

   (c) Can you guess the smallest pair of numbers requiring 8 Euclidean algorithm steps?

   (d) Is there a pattern here? Do the numbers which keep coming up have a name?

(a) $14 \equiv 20 \bmod 8$

$20 = (18 \times 1) + 2$

$14 = (18 \times 1) - 4 \rightsquigarrow$ FALSE

(b) $-15/3 = -5$

$3 = (3 \times 1) + 0$

$-15 = (3 \times -5) + 0 \rightsquigarrow$ TRUE

(c) $-11 \equiv (\bmod 3$

$1 \doteq (-3 \times 3) - 2$

$1 = (3 \times 3) - 2 \rightsquigarrow$ TRUE

(d) 9 is NOT prime

↳ $3 \times 3 = 9$

↳ $9 \times 1 = 9$

↳ $18/2 = 9 \rightsquigarrow$ FALSE

(e) $1000 \equiv 12544 \bmod 5$ $\rightsquigarrow$ FALSE

$$\begin{array}{r} 200 \\ 5\overline{)1000} \\ \underline{10} \\ 00 \end{array} \qquad 5\overline{)12544}$$

↳ 12544 cannot divide by 5 due to 12544 being even $\rightsquigarrow$ FALSE

(f) 66 divides 22

$66 = (22 \times 3) + 2$

$22 = (22 \times 1) + 0$

} 22 cannot be divided by 66 $\Rightarrow 22 = (0 \times 66) + 22$

$66 = (1 \times 66) + \underline{\underline{0}}$

2) Euclidean algorithm :

(a) GCD of 1022, 400

$1022 = 2(400) + 222$

$400 = 1(222) + 178$

$222 = 1(178) + 44$

$178 = 4(44) + 2$

$44 = 22(2) + 0$

GCD of 1022, 400 is 2 #

(b) Find a and b where $\gcd(1022, 400) = a(1022) + b(400)$

$2 = 178 - 4(44)$

$2 = 178 - 4(222 - 178)$

$2 = 5(178) - 4(222)$

$2 = 5(400 - 222) - 4(1022 - 2(400))$

$2 = 5(400) - 5(222) - 4(1022 - 2(400))$

$2 = 5(400) - 5(1022 - 2(400)) - 4(1022) + 8(400)$

$2 = 13(400) - 4(1022) - 5(1022) + 10(400)$

$2 = 23(400) - 9(1022)$

* $a = -9,\ b = 23$

(c) Find a and b such that $8 = a(1022) + b(400)$

$2 = 23(400) - 9(1022)$ $8 = 4 \times 2$

$4 \times 2 = [23(400) - 9(1022)] \times 4$

$8 = 92(400) - 36(1022)$

$\therefore a = -36 ; b = 92$

3)(a) n = integer

x (smallest integer) ≥ 2, $n | x$; must x be prime?

x must be prime, if $x \neq$ prime then there can be the existance of c where $2 \leq c < x$ so where c can divide x so it can also divide by n hence c can be smallest integer.

(b) y = integer $\Rightarrow y \equiv 2 \bmod 3$

integer $z : 0 \leq z \leq 11$

is $y \equiv z \pmod{12}$ possible?

$y \equiv 2 \bmod 3 \Rightarrow y = 2 + 3k \longrightarrow 3k = y - 2$

$y \equiv z \bmod 12 \Rightarrow y = z + 12k \longrightarrow 12k = y - z$

For some int l, k is $4l, 4l+1, 4l+2, 4l+3$

if $k = 4l \Rightarrow y = 2 + 3(4l)$

$y = 2 + 12l \rightsquigarrow 2$, within z range

if $k = 4l+1 \Rightarrow y = 2 + 3(4l+1)$

$y = 2 + 12l + 3$

$y = 12l + 5 \rightsquigarrow 5$, within z range

if $k = 4l+2 \Rightarrow y = 2 + 3(4l+2)$

$y = 2 + 12l + 6$

$y = 12l + 8 \rightsquigarrow 8$, within z range

if $k = 4l+3 \Rightarrow y = 2 + 3(4l+3)$

$y = 2 + 12l + 9$

$y = 12l + 11 \rightsquigarrow 11$, within z range

* y might be congruent to 2, 5, 8, 11, 12