CS 70 Discrete Mathematics and Probability Theory
Fall 2018 Alistair Sinclair and Yun Song

DIS 3B

1 Divisible or Not

(a) Prove that for any number n, the number formed by the last two digits of n are divisible by 4 if and only if n is divisible by 4. (For example, '23xx' is divisible by 4 if and only if the number 'xx' is divisible by 4.)

(b) Prove that for any number n, the sum of the digits of n are divisible by 3 if and only if n is divisible by 3.

2 Extended Euclid

In this problem we will consider the extended Euclid's algorithm. The bolded numbers below keep track of which numbers appeared as inputs to the gcd call. Remember that we are interested in writing the GCD as a linear combination of the original inputs, so we don't want to accidentally simplify the expressions and eliminate the inputs.

(a) Note that x mod y, by definition, is always x minus a multiple of y. So, in the execution of Euclid's algorithm, each newly introduced value can always be expressed as a "combination" of the previous two, like so:

$$\begin{aligned}
\gcd(2328,440) &= \gcd(440,128) && [\mathbf{128} = 1\times\mathbf{2328} + (-5)\times\mathbf{440}]\\
&= \gcd(128,56) && [\mathbf{56} = 1\times\mathbf{440} + \underline{\text{-3}}\times\mathbf{128}]\\
&= \gcd(56,16) && [\mathbf{16} = 1\times\mathbf{128} + \underline{\text{-2}}\times\mathbf{56}]\\
&= \gcd(16,8) && [\mathbf{8} = 1\times\mathbf{56} + \underline{\text{-3}}\times\mathbf{16}]\\
&= \gcd(8,0) && [\mathbf{0} = 1\times\mathbf{16} + (-2)\times\mathbf{8}]\\
&= 8.
\end{aligned}$$

(Fill in the blanks)

(b) Now working back up from the bottom, we will express the final gcd above as a combination of the two arguments on each of the previous lines:

$$\begin{aligned} 8 &= 1 \times \mathbf{8} + 0 \times \mathbf{0} = 1 \times \mathbf{8} + (1 \times \mathbf{16} + (-2) \times \mathbf{8}) \\ &= 1 \times \mathbf{16} - 1 \times \mathbf{8} \\ &= \underline{\text{-1}} \times \mathbf{56} + \underline{\text{4}} \times \mathbf{16} \end{aligned}$$

[*Hint*: Remember, $\mathbf{8} = 1 \times \mathbf{56} + (-3) \times \mathbf{16}$. Substitute this into the above line.]

$$= \underline{\text{4}} \times \mathbf{128} + \underline{\text{-9}} \times \mathbf{56}$$

[*Hint*: Remember, $\mathbf{16} = 1 \times \mathbf{128} + (-2) \times \mathbf{56}$.]

$$\begin{aligned} &= \underline{\text{-9}} \times \mathbf{440} + \underline{\text{31}} \times \mathbf{128} \\ &= \underline{\text{31}} \times \mathbf{2328} + \underline{\text{-164}} \times \mathbf{440} \end{aligned}$$

(c) In the same way as just illustrated in the previous two parts, calculate the gcd of 17 and 38, and determine how to express this as a "combination" of 17 and 38.

gcd(17, 38) = 1 = 9*17 - 4*38

(d) What does this imply, in this case, about the multiplicative inverse of 17, in arithmetic mod 38?

17^-1 = 9

3 Modular Arithmetic Equations

Solve the following equations for x and y modulo the indicated modulus, or show that no solution exists. Show your work.

(a) $9x \equiv 1 \pmod{11}$.

9^-1 = 5 (mod 11) —> x = 5 (unique inverse)

(b) $10x + 23 \equiv 3 \pmod{31}$.

10x === 11 (mod 31)
10^-1 = 28
—> x === 28*11 = 308 === 29 (mod 31) unique inverse

(c) $3x + 15 \equiv 4 \pmod{21}$.

3x === 10 (mod 21)
but gcd(3,21) = 3, so always multiple of 3, no solution

(d) The system of simultaneous equations $3x + 2y \equiv 0 \pmod{7}$ and $2x + y \equiv 4 \pmod{7}$.

-x === -8 (mod 7) —> x === 8 === 1 (mod 7)
—> y === 2 (mod 7)