# COT 3100 Homework #3 Solutions

1) (5 pts) State the quotient and remainder when dividing by b for each of the following examples:

a) a = 132, b = 15
132 = 8 x 15 + 12, thus **q = 8, r = 12**

b) a = 54321, b = 232
54321 = 234 x 232 + 33, thus **q = 234, r = 33**

c) a = 177, b = 296
177 = 0 x 296 + 177, thus **q = 0, r = 177**

d) a = 396, b = 83
396 = 4 x 83 + 64, thus **q = 4, r = 64**

e) a = 212, b = 173
212 = 1 x 173 + 39, thus **q = 1, r = 39**

2) (6 pts) Using the method of calculating remainders for one full cycle of exponents, find the remainders when dividing a by b for each of the following examples:

1) $a = 10^{15}$, b = 7

| exp | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| $a^{exp}$ mod b | 1 | 3 | 2 | 6 | 4 | 5 | 1 |

$10^{15} \equiv 10^3(10^6)^2 \equiv 6(1)^2 \equiv 6(1) \equiv \mathbf{6} \pmod 7$

2) $a = 15^{21}$, b = 11

| exp | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| $a^{exp}$ mod b | 1 | 4 | 5 | 9 | 3 | 1 |

$15^{21} \equiv 15^1(10^5)^4 \equiv 4(1)^4 \equiv 4(1) \equiv \mathbf{4} \pmod{11}$

3) $a = 23^{30}$, b = 9

| exp | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| $a^{exp}$ mod b | 1 | 5 | 7 | 8 | 4 | 2 | 1 |

$23^{30} \equiv 23^6(23^6)^4 \equiv 1(1)^4 \equiv 1(1) \equiv \mathbf{1} \pmod 9$

3) (6 pts) Using the method of fast modular exponentiation (either top down or bottom up), find the remainders when dividing a by b for each of the following examples:

1) a = $4^{27}$, b = 19

| exp | 0 | 1 | 2 | 4 | 8 | 16 |
|---|---|---|---|---|---|---|
| $a^{exp}$ mod b | 1 | 4 | -3 | 9 | 5 | 6 |

$$\begin{aligned} 4^{27} &\equiv (4^{16})(4^{8})(4^{2})(4^{1}) \\ &\equiv 6 \times 5 \times (-3) \times 4 \\ &\equiv (30) \times (-12) \\ &\equiv 11 \times 7 \\ &\equiv \mathbf{1} \bmod 19 \end{aligned}$$

2) a = $3^{31}$, b = 17

| exp | 0 | 1 | 2 | 4 | 8 | 16 |
|---|---|---|---|---|---|---|
| $a^{exp}$ mod b | 1 | 3 | 9 | -4 | -1 | 1 |

$$\begin{aligned} 3^{31} &\equiv (3^{16})(3^{8})(3^{4})(3^{2})(3^{1}) \\ &\equiv (1)(-1)(-4)(9)(3)(1) \\ &\equiv (36)(3) \bmod 17 \\ &\equiv (2)(3) \bmod 17 \\ &\equiv \mathbf{6} \bmod 17 \end{aligned}$$

4) (16 pts) Use the Euclidean Algorithm, showing every step, to calculate each of the following greatest common divisors (gcd).

1) gcd(384, 126)

$$384 = 3 * 126 + 6$$
$$126 = 21 * 6$$

Thus, gcd(384, 126) = 6

2) gcd(144, 89)

$$144 = 1 * 89 + 55$$
$$89 = 1 * 55 + 34$$
$$55 = 1 * 34 + 21$$
$$34 = 1 * 21 + 13$$
$$21 = 1 * 13 + 8$$
$$13 = 1 * 8 + 5$$
$$8 = 1 * 5 + 3$$
$$5 = 1 * 3 + 2$$
$$3 = 1 * 2 + 1$$
$$2 = 2 * 1$$

Thus, gcd(144, 89) = 1

3) gcd(221, 78)

$221 = 2 * 78 + 65$
$78 = 1 * 65 + 13$
$65 = 5 * 13$
Thus, gcd(221, 78) = 13

4) gcd(1105, 767)

$1105 = 1 * 767 + 338$
$767 = 2 * 338 + 91$
$338 = 3 * 91 + 65$
$91 = 1 * 65 + 26$
$65 = 2 * 26 + 13$
$26 = 2 * 13$
Thus, gcd(1105, 767) = 13

5) (5 pts) Determine, with proof, all ordered pairs of integers (x, y) which satisfy the equation

$$1001x + 728y = 12345$$

1001 = 1 * 728 + 273
728 = 2 * 273 + 182
273 = 1 * 182 + 91
182 = 2 *91, thus, gcd(1001, 728) = 91

Notice however, that 12345 is NOT divisible by 91. (The remainder when you do the division is 60.)

It follows that since the left hand side is always divisible by 91 and the right hand side is not, there are no integer solutions (x, y) to the equation.

6) (7 pts) Let x and y be integers such that $7 \mid (3x + 5y)$. Prove that $7 \mid (16x + 29y)$

Using the given information that 7 | (3x + 5y), there exists an integer c such that (3x+5y) = 7c.

16x + 29y = (7x + 9x) + (14y + 15y)
= 7x + 14y + (9x + 15y)
= 7x + 14y + 3(3x + 5y)
= 7x + 14y + 3(7c), using given information
= 7(x + 2y + 3c)

Since x, y and c are integers, it follows that x + 2y + 3c is also an integer. Thus, we've proven that 7 | (16x + 29y).

To ascertain the multiples of 7x and 7y that need to be "split off" in a more formulaic way, we could set up the following equation:

$16x + 29y = 7ax + 7by + c(3x + 5y)$, where a, b and c are integers

Our goal is to find values of a, b and c that satisfy this equation.

Equating coefficients, we find $16 = 7a + 3c$
$29 = 7b + 5c$

Multiply the first equation through by 5, and the second by 3 and solve for 15c.

Solving for 15c, we find $15c = 5(16 – 7a) = 3(29 – 7b)$.

$80 – 35a = 87 – 21b$
$35a – 21b = 7$
$5a – 3b = 1$, we can eyeball a solution $a = 1, b = 2$. (Any solution suffices for our purposes.)

Alternatively, we can run the Extended Euclidean Algorithm:

$5 = 1 \times 3 + 2$
$3 = 1 \times 2 + 1$

$3 – 2 = 1$
$3 – (5 – 3) = 1$
$2 \times 3 – 1 \times 5 = 1$, and here we have the solution $a = -1, b = 2$ for $5a + 3b = 1$.
It follows that $c = (16 – 7(1))/3 = 3$.

Either way, this allows us to discover, in a formulaic way, that

$16x + 29y = 7x + 14y + 3(3x + 5y)$.

Then, we can complete the proof as previously shown.

7) (5 pts) Give a summary of the life and mathematical contributions of Shafi Goldwasser.

Shafi Goldwasser is a New York City-born computer scientist who graduated with her degree from Carnegie Mellon University, followed by a PhD in computer science from UC Berkeley. In her career she has worked as a professor through multiple universities and developed advancements to cryptography, number theory, and complexity theory.

As a member of the theory of computation group at MIT CS and AI Laboratory, Goldwasser received the 2012 Turing Award during her time as a professor at the Institution. In addition to her impressive professorship at MIT, she is also a professor at the Weizmann Institute of Science, director of the Simons Institute for the Theory of Computing at UC Berkeley, and chief scientist and co-founder of the company Duality Technologies. She has offered her knowledge and research of Zero Knowledge Blockchain and Algorand, her specialty, and is recognized as the co-inventor of zero-knowledge proofs, an integral aspect of cryptographic and blockchain technology.

In addition to the Turing Award in 2012, she has won the Godel Prize twice, the ACM Grace Murray Hopper Award, the RSA Award for Excellence in Mathematics, the Athena Lecturer Award, The Franklin Institute's Benjamin Franklin Medal, the IEEE Emanuel R. Piore Award, the Frontier of Knowledge award, the Suffrage Science award, and the L'Oreal-UNESCO for Women in Science Award, over the last thirty years or so. She has also been elected to multiple academies and was awarded an honorary doctorate by the University of Oxford.

Source: https://en.wikipedia.org/wiki/Shafi_Goldwasser