CS 2050 Fall 2022 Homework 6

Due: March 10th

Released: March 3rd

i. This assignment is due on **11:59 PM EST, Friday, October 14, 2022**. Early submissions (24+ hours in advance) receive 2.5 points of extra credit. You may turn it in one day late for a 10 point penalty or two days late for a 25 point penalty. Assignments more than two days late will NOT be accepted. We will prioritize on-time submissions when grading before an exam.

ii. You will submit your assignment on **Gradescope**. Shorter answers may be entered directly into response fields, however longer answer must be recorded on a typeset (e.g. using LaTeX) or *neatly* written PDF.

iii. Ensure that all questions are correctly assigned on Gradescope. Questions that take up multiple pages should have all pages assigned to that question. Incorrect page assignments can lead to point deductions.

iv. You may collaborate with other students, but any written work should be your own. Write the names of the students you work with on the top of your assignment.

v. Always justify your work, even if the problem doesn't specify it. It can help the TA's to give you partial credit.

Author(s): Ronnie Howard

1. (3 points each) Find the prime factorization of each of the following integers.

   a) $46^2 26^2 15^3$

      $2^4 3^3 5^3 13^2 23^2$

   b) $8!$

      $2^7 3^2 5^1 7^1$

2. (4 points) Approximate the number of primes whose cubed root does not exceed 8. Round to the nearest integer. Show your work.

$$2 \leq n < 8^3$$

$$2 \leq n < 512$$

Per the Prime Number Theorem, the fraction of prime numbers between 2 and n is $\frac{1}{\ln(n)}$ so the fraction of prime numbers between 2 and 512 is $\frac{1}{\ln(512)} = 0.1803$. Multiplying by the range of numbers, we get an estimate of 82 primes ($\frac{512}{\ln(512)} = 82.073 \approx 82$).

3. (4 points each) Convert the decimal expansion for 321 into a binary expansion. Show your work for full credit.

$1 \ldots 321\%2 = 1$
$\ldots . \lfloor \frac{321}{2} \rfloor = 160$
$0 \ldots 160\%2 = 0$
$\ldots . \lfloor \frac{160}{2} \rfloor = 80$
$0 \ldots 80\%2 = 0$
$\ldots . \lfloor \frac{80}{2} \rfloor = 40$
$0 \ldots 40\%2 = 0$
$\ldots . \lfloor \frac{40}{2} \rfloor = 20$
$0 \ldots 20\%2 = 0$
$\ldots . \lfloor \frac{20}{2} \rfloor = 10$
$0 \ldots 10\%2 = 0$
$\ldots . \lfloor \frac{10}{2} \rfloor = 5$
$1 \ldots 5\%2 = 1$
$\ldots . \lfloor \frac{5}{2} \rfloor = 2$
$0 \ldots 2\%2 = 0$
$\ldots . \lfloor \frac{2}{2} \rfloor = 1$
$1 \ldots 1\%2 = 1$
$\ldots . \lfloor \frac{1}{2} \rfloor = 0$

1 0 1 0 0 0 0 0 1
$(10100\ 0001)_2$

4. (4 points each) Convert the binary expansion of $(10100110)_2$ into an octal, hexadecimal and decimal expansion. Show your work for full credit.

Octal:$10100110 \ = \ 10\,100\,110 \ = \ 010\,100\,110 \ = \ 2\,4\,6 \ = \ 246$
Hexadecimal: $10100110 \ = \ 1010\,0110 = \ 1010\,0110 \ = \ A\,6 \ = \ A6$
Decimal:

$$0 * 1 = 0$$

$$1 * 2 = 2$$

$$1 * 4 = 4$$

$$0 * 8 = 0$$

$$0 * 16 = 0$$

$$1 * 32 = 32$$

$$0 * 64 = 0$$

$$1 * 128 = 128$$

$$0 + 2 + 4 + 0 + 0 + 32 + 0 + 128 = 166$$

5. (4 points each) Convert the hexadecimal expansion $(C9A6)_{16}$ into a binary expansion. Show your work for full credit.

$$C9A6$$

$$C \quad 9 \quad A \quad 6$$

$$12 \quad 9 \quad 10 \quad 6$$

$$1100 \quad 1001 \quad 1010 \quad 0110$$

$$(1100\,1001\,1010\,0110)_2$$

6. (4 points each) Convert the hexadecimal expansion $(BA13)_{16}$ into an octal expansion. Show your work for full credit.

$$BA13$$

$$B \quad A \quad 1 \quad 3$$

$$11 \quad 10 \quad 1 \quad 3$$

$$1011 \quad 1010 \quad 0001 \quad 0011$$

$$1011101000010011$$

$$(001\,011\,101\,000\,010\,011)_8$$

7. (4 points each) Evaluate the following. Note: a calculator is not needed for these problems, and similar difficulty problems may appear on the exam (where a calculator is not permitted).

   (a) $(43^2 \bmod 36) \bmod 8$

$$
\begin{aligned}
&(43^2 \bmod 36) \bmod 8 \\
&= (((43 \bmod 36)(43 \bmod 36)) \bmod 36) \bmod 8 \\
&= (((7)(7)) \bmod 36) \bmod 8 \\
&= (49 \bmod 36) \bmod 8 \\
&= 13 \bmod 8 \\
&= 5
\end{aligned}
$$

   (b) $(9^3 \bmod 11)^2 \bmod 18$

$$
\begin{aligned}
&(9^3 \bmod 11)^2 \bmod 18 \\
&= (((9 \bmod 11)(9 \bmod 11)(9 \bmod 11)) \bmod 11)^2 \bmod 18 \\
&= (((-2)(-2)(-2) \bmod 11)^2 \bmod 18 \\
&= (-8 \bmod 11)^2 \bmod 18 \\
&= (3)^2 \bmod 18 \\
&= 9 \bmod 18 \\
&= 9
\end{aligned}
$$

   (c) $(24^2 \bmod 6) \bmod 7003$

$$
\begin{aligned}
&(24^2 \bmod 6) \bmod 7003 \\
&= (((24 \bmod 6)(24 \bmod 6)) \bmod 6) \bmod 7003 \\
&= (((0)(0)) \bmod 6) \bmod 7003 \\
&= (0 \bmod 6) \bmod 7003 \\
&= 0 \bmod 7003 \\
&= 0
\end{aligned}
$$

(d) $((-7)^3 \bmod 10)^3 \bmod 5$

$$
\begin{aligned}
&((-7)^3 \bmod 10)^3 \bmod 5 \\
&= ((((-7) \bmod 10)((-7) \bmod 10)((-7) \bmod 10))) \bmod 10)^3 \bmod 5 \\
&= (((3)(3)(3)) \bmod 10)^3 \bmod 5 \\
&= (27 \bmod 10)^3 \bmod 5 \\
&= (7)^3 \bmod 5 \\
&= ((7 \bmod 5)(7 \bmod 5)(7 \bmod 5)) \bmod 5 \\
&= ((2)(2)(2)) \bmod 5 \\
&= (8) \bmod 5 \\
&= 3
\end{aligned}
$$

8. (3 points each) Suppose $a \equiv_{15} 2$ and $b \equiv_{15} 11$ for $a, b \in \mathbb{Z}$. Find the integer c such that $0 \le c \le 14$ in each of the following modular congruences. Note: a calculator is not needed for these problems, and similar difficulty problems may appear on the exam (where a calculator is not permitted).

(a) $c \equiv_{15} 11b$

(1)	$a, b \in \mathbb{Z}$	Given
(2)	$a = 15k_1 + 2, \quad k_1 \in \mathbb{Z}$	Given
(3)	$b = 15k_2 + 11, \quad k_2 \in \mathbb{Z}$	Given
(4)	$0 \le c \le 14, \quad c \in \mathbb{Z}$	Given
(5)	$c \bmod 15 = 11b \bmod 15$	Given
(6)	$c \bmod 15 = (11(15k_2 + 11)) \bmod 15$	Substitute (3) into (5)
(7)	$c \bmod 15 = (11 * 15k_2 + 11 * 11) \bmod 15$	Multiplication Distributive (6)
(8)	$c \bmod 15 = ((11 * 15k_2) \bmod 15 + 121 \bmod 15) \bmod 15$	Mod Multiplicative Property (7)
(9)	$c \bmod 15 = (((11 \bmod 15)$ $(15k_2 \bmod 15)) \bmod 15 + 121 \bmod 15) \bmod 15$	Mod Multiplicative Property (8)
(10)	$c \bmod 15 = (((11 \bmod 15)((15 \bmod 15)$ $(k_2 \bmod 15) \bmod 15)) \bmod 15 + 121 \bmod 15) \bmod 15$	Mod Multiplicative Property (9)
(11)	$c \bmod 15 = (((11 \bmod 15)((0)$ $(k_2 \bmod 15) \bmod 15)) \bmod 15 + 121 \bmod 15) \bmod 15$	Simplification (10)
(12)	$c \bmod 15 = (((11 \bmod 15)(0)$ $\bmod 15)) \bmod 15 + 121 \bmod 15) \bmod 15$	Simplification (11)
(13)	$c \bmod 15 = ((0 \bmod 15) \bmod 15 +$ $121 \bmod 15) \bmod 15$	Simplification (12)
(14)	$c \bmod 15 = (0 \bmod 15 + 121 \bmod 15) \bmod 15$	Simplification (13)
(15)	$c \bmod 15 = 121 \bmod 15 \bmod 15$	Simplification (14)
(16)	$c \bmod 15 = 1 \bmod 15$	Simplification (15)
(17)	$c \bmod 15 = 1$	Simplification (16)
(18)	$c = 15k_3 + 1, \quad k_3 \in \mathbb{Z}$	Definition of congruence (17)
(19)	$0 \le 15k_3 + 1 \le 14$	Substitute (18) into (4)
(20)	$-1 \le 15k_3 \le 13$	Simplify (19)
(21)	$\frac{-1}{15} \le k_3 \le \frac{13}{15}$	Divide 15 (20)
(22)	$k_3 = 0$	k_3 is integer (21)
(23)	$c = 1$	Substitute (22) into (18)

(b) $c \equiv_{15} a^3 + 2b^2$

(1)	$a, b \in \mathbb{Z}$	Given
(2)	$a = 15k_1 + 2, \quad k_1 \in \mathbb{Z}$	Given
(3)	$b = 15k_2 + 11, \quad k_2 \in \mathbb{Z}$	Given
(4)	$0 \leq c \leq 14, \quad c \in \mathbb{Z}$	Given
(5)	$c \bmod 15 = (a^3 + 2b^2) \bmod 15$	Given
(6)	$c \bmod 15 = (a^3 \bmod 15 + 2b^2 \bmod 15) \bmod 15$	Property of Mods
(7)	$c \bmod 15 = ((15k_1 + 2)^3 \bmod 15 + 2b^2 \bmod 15) \bmod 15$	Substitute (2) into (6)
(8)	$c \bmod 15 = (2^3 \bmod 15 + 2b^2 \bmod 15) \bmod 15$	Simplify (7)
(9)	$c \bmod 15 = (8 + (2b^2 \bmod 15)) \bmod 15$	Simplify (8)
(10)	$c \bmod 15 = (8 + (2(15k_2 + 11)^2 \bmod 15)) \bmod 15$	Substitute (3) into (10)
(11)	$c \bmod 15 = (8 + ((2 * 121) \bmod 15)) \bmod 15$	Simplify (10)
(12)	$c \bmod 15 = (8 + (2 \bmod 15)) \bmod 15$	Simplify (11)
(13)	$c \bmod 15 = (10 \bmod 15$	Simplify (12)
(14)	$c \bmod 15 = 10$	Simplify (13)
(15)	$c = 15k_3 + 10, \quad k_3 \in \mathbb{Z}$	Definition of congruence (14)
(16)	$0 \leq 15k_3 + 10 \leq 14$	Substitute (15) into (4)
(17)	$-10 \leq 15k_3 \leq 4$	Simplify (16)
(18)	$\frac{-10}{15} \leq k_3 \leq \frac{4}{15}$	Divide 15 (17)
(19)	$k_3 = 0$	k_3 is integer (18)
(20)	$c = 10$	Substitute (18) into (15)

(c) $c \equiv_{15} (8a)^{2000}$

(1)	$a, b \in \mathbb{Z}$	Given
(2)	$a = 15k_1 + 2, \quad k_1 \in \mathbb{Z}$	Given
(3)	$b = 15k_2 + 11, \quad k_2 \in \mathbb{Z}$	Given
(4)	$0 \leq c \leq 14, \quad c \in \mathbb{Z}$	Given
(5)	$c \bmod 15 = ((8a)^{2000}) \bmod 15$	Given
(6)	$c \bmod 15 = ((8(15k_1 + 2))^{2000}) \bmod 15$	Property of Mods
(6)	$c \bmod 15 = (120k_1 + 16)^{2000}) \bmod 15$	Property of Mods
(6)	$c \bmod 15 = ((0 + 1))^{2000}) \bmod 15$	Property of Mods
(6)	$c \bmod 15 = (1^{2000}) \bmod 15$	Property of Mods
(6)	$c \bmod 15 = 1 \bmod 15$	Property of Mods
(6)	$c \bmod 15 = 1$	Property of Mods
(7)	$c = 15k_3 + 1, \quad k_3 \in \mathbb{Z}$	Definition of congruence (6)
(8)	$0 \leq 15k_3 + 1 \leq 14$	Substitute (7) into (4)
(9)	$-1 \leq 15k_3 \leq 13$	Simplify (8)
(10)	$\frac{-1}{15} \leq k_3 \leq \frac{13}{15}$	Divide 15 (9)
(11)	$k_3 = 0$	k_3 is integer (10)
(12)	$c = 1$	Substitute (11) into (7)

9. (8 points) Prove that if $a|b$ and $b|a$ then $b = a$ or $b = -a$

   Prove using direct proof, if $a|b$ and $b|a$ then $b = a$ or $b = -a$

1.	$a = k_1 b, \quad k_1 \in \mathbb{Z}$	(Given, Definition of Divisibility)
2.	$b = k_2 a, \quad k_2 \in \mathbb{Z}$	(Given, Definition of Divisibility)
3.	$a = k_1(k_2 a)$	(Substitute (2) into (1))
4.	$1 = k_1 k_2$	(Divide both sides of (3) by a)
5.	$k_1, k_2 = \pm 1$	((4) with k_1, k_2 being integers from (1), (2))
6.	$b = \pm a$	(Substitute k_2 from (5) into (2))
7.	$b = a$ or $b = -a$,	(Definition of $\pm$ (6))

   By (1), (2), (7), we have proved using direct proof that if $a|b$ and $b|a$ then $b = a$ or $b = -a$.

10. (10 points each) Use the sieve of Eratosthenes to find all prime numbers less than 115. You must show work.

$$\begin{bmatrix}
\cancel{1} & 2 & 3 & \cancel{4} & 5 & \cancel{6} & 7 & \cancel{8} & \cancel{9} & \cancel{10} \\
11 & \cancel{12} & 13 & \cancel{14} & \cancel{15} & \cancel{16} & 17 & \cancel{18} & 19 & \cancel{20} \\
\cancel{21} & \cancel{22} & 23 & \cancel{24} & \cancel{25} & \cancel{26} & \cancel{27} & \cancel{28} & 29 & \cancel{30} \\
31 & \cancel{32} & \cancel{33} & \cancel{34} & \cancel{35} & \cancel{36} & 37 & \cancel{38} & \cancel{39} & \cancel{40} \\
41 & \cancel{42} & 43 & \cancel{44} & \cancel{45} & \cancel{46} & 47 & \cancel{48} & \cancel{49} & \cancel{50} \\
\cancel{51} & \cancel{52} & 53 & \cancel{54} & \cancel{55} & \cancel{56} & \cancel{57} & \cancel{58} & 59 & \cancel{60} \\
61 & \cancel{62} & \cancel{63} & \cancel{64} & \cancel{65} & \cancel{66} & 67 & \cancel{68} & \cancel{69} & \cancel{70} \\
71 & \cancel{72} & 73 & \cancel{74} & \cancel{75} & \cancel{76} & \cancel{77} & \cancel{78} & 79 & \cancel{80} \\
\cancel{81} & \cancel{82} & 83 & \cancel{84} & \cancel{85} & \cancel{86} & \cancel{87} & \cancel{88} & 89 & \cancel{90} \\
\cancel{91} & \cancel{92} & \cancel{93} & \cancel{94} & \cancel{95} & \cancel{96} & 97 & \cancel{98} & \cancel{99} & \cancel{100} \\
101 & \cancel{102} & 103 & \cancel{104} & \cancel{105} & \cancel{106} & 107 & \cancel{108} & 109 & \cancel{110} \\
\cancel{111} & \cancel{112} & 113 & \cancel{114} & & & & & &
\end{bmatrix}$$

$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113$

11. (3 points each) Identify the GCD of the following group of numbers.

    a) -294, 274

$$-294 = (-1)(2)(3)(7^2)$$
$$274 = (2)(137)$$
$$\gcd(-294, 274) = 2$$

b) $2^6 3^2 5^4 7^2$, $2^3 3^4 7$

$$2^6 3^2 5^4 7^2$$
$$2^3 3^4 7$$
$$\gcd(2^6 3^2 5^4 7^2, 2^3 3^4 7) = 2^3 3^2 7 = 504$$

12. (2 points each) Identify the LCM of the following group of numbers.

a) 77, 336

$$77 = (7)(11)$$
$$336 = (2^4)(3)(7)$$
$$\text{lcm}(77, 336) = (2^4)(3)(7)(11) = 3696$$

b) $3^4 5^6 11^2$, $2^4 5^3 13$

$$3^4 5^6 11^2$$
$$2^4 5^3 13$$
$$\text{lcm}(3^4 5^6 11^2, 2^4 5^3 13) = (2^4)(3^4)(5^6)(11^2)(13) = 31853250000$$

13. (2 points each) Determine whether the following sets of integer are pairwise relatively prime.

a) $\{15, 175, 39\}$

$$15 = (3)(5)$$
$$175 = (5^2)(7)$$
$$39 = (3)(13)$$
$$\gcd(15, 175) = 5 \neq 1$$

Pairwise not relatively prime as the pair $\gcd(15, 175)$ is not 1.

b) $\{63, 50, 17\}$

$$63 = (3^2)(7)$$
$$50 = (2)(5^2)$$
$$17 = (17)$$
$$\gcd(63, 50) = 1$$
$$\gcd(63, 17) = 1$$
$$\gcd(50, 17) = 1$$

All combinations of GCD pairs are 1 so the set of integers are relatively prime.

14. (4 points each) Use the Euclidean algorithm to find the following values. You must clearly show all steps of your work using the Euclidean algorithm taught in class.

 a) $\gcd(123, 456)$

 1. $456 = 3 * 123 + 87$
 2. $123 = 1 * 87 + 36$
 3. $87 = 2 * 36 + 15$
 4. $36 = 2 * 15 + 6$
 5. $15 = 2 * 6 + 3$
 6. $6 = 2 * 3 + 0$
 8. $\gcd(123, 456) = 3$ (Euclid's Algorithm)

 b) $\gcd(423, 72)$

 1. $423 = 5 * 72 + 63$
 2. $72 = 1 * 63 + 9$
 3. $63 = 7 * 9 + 0$
 8. $\gcd(423, 72) = 9$ (Euclid's Algorithm)

15. (3 points each) Use Euler's Totient Function (show work) to calculate the number of integers that are relatively prime and less than each of the following integers:

 a) 22

 prime factors of 22 is 2, 11

$$\phi(22) = 22(1 - \frac{1}{2})(1 - \frac{1}{11}) = 22(\frac{1}{2})(\frac{10}{11}) = 10$$

 b) 23

 prime factor of 23 is 23

$$\phi(23) = 23(1 - \frac{1}{23}) = 23(\frac{22}{23}) = 22$$

 b) 24

 prime factor of 24 is 2,3

$$\phi(24) = 24(1 - \frac{1}{2})(1 - \frac{1}{3}) = 24(\frac{1}{2})(\frac{2}{3}) = 8$$