MATH 55 - HOMEWORK 4 SOLUTIONS

Exercise 0.1. 4.3 - 4(a,e,f)

Proof. (a) $39 = 3 \cdot 13$
(e) $111 = 3 \cdot 37$
(f) $143 = 11 \cdot 13$. □

Exercise 0.2. 4.3 - 11

Proof. Suppose $\log_2 3 = \frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $b \neq 0$. As $2^1 < 3$ we know $\log_2 3 \geq 1$ so we may assume a, b are both positive. Then $3 = 2^{\frac{a}{b}}$ so by exponentiating both sides by b, we have

$$3^b = 2^a.$$

But as 2 and 3 are relatively prime (in fact, prime), we must have $a = b = 0$, against our assumption. This contradiction proves $\log_2 3$ is irrational. □

Exercise 0.3. 4.3 - 16(a,d)

Proof. We can show these sets of numbers are relatively prime by computing their prime factorizations and noticing that they have no factors in common.
(a) $21, 34$, and 55 are relatively prime as these are their prime factorizations:

$$\begin{aligned} 21 &= 3 \cdot 7 \\ 34 &= 2 \cdot 17 \\ 55 &= 5 \cdot 11. \end{aligned}$$

(d) 17, 18, 19, and 23 are relatively prime as 17, 19, and 23 are prime, while $18 = 2 \cdot 3^2$, so these numbers have no prime factors in common. □

Exercise 0.4. 4.3 - 28

Proof. First we find the prime factorization of 1000 and 625:

$$\begin{aligned} 1000 &= 2^3 5^3 \\ 625 &= 5^4. \end{aligned}$$

From this, it follows that $\gcd(1000, 625) = 5^3 = 125$ and $\text{lcm}(1000, 625) = 2^3 5^4 = 5000$. It is now easy to check $125 \cdot 5000 = 1000 \cdot 625$. □

Exercise 0.5. 4.3 - 32

Proof. (a) Clearly $\gcd(1, 5) = 1$
(b) $\gcd(101, 100) = \gcd(1, 100) = 1$ as $101 = 100 + 1$.
(c) $\gcd(123, 277) = \gcd(123, 31) = \gcd(31, 30) = \gcd(1, 30) = 1$, using the following equations:

$$\begin{aligned} 277 &= 2 \cdot 123 + 31 \\ 123 &= 3 \cdot 31 + 30 \\ 31 &= 30 + 1. \end{aligned}$$

□

Exercise 0.6. 4.3 - 40

Proof. (a) Euclid's algorithm gives

$$\begin{aligned} 11 &= 9 + 2 \\ 9 &= 4 \cdot 2 + 1 \end{aligned}$$

Then we get $1 = 9 - 4 \cdot 2$ and $2 = 11 - 9$ so

$$1 = 9 - 4 \cdot (11 - 9) = 5 \cdot 9 - 4 \cdot 11.$$

(b) Euclid's algorithm gives

$$44 = 33 + 11$$

and $33 = 3 \cdot 11$, so $11 = \gcd(44, 33)$ and we have $11 = 44 - 33$.

Date: February 17, 2016.

(c) Euclid's algorithm gives

$$\begin{aligned} 78 &= 2 \cdot 35 + 8 \\ 35 &= 4 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 2 + 1. \end{aligned}$$

Solving for the remainder and substituting in working from the bottom, we get

$$\begin{aligned} 1 = 3 - 2 &= 3 \cdot 3 - 8 \\ &= 3 \cdot (35 - 4 \cdot 8) - 8 \\ &= 3 \cdot 35 - 13 \cdot 8 \\ &= 3 \cdot 35 - 13(78 - 2 \cdot 35) \\ &= 29 \cdot 35 - 13 \cdot 78. \end{aligned}$$

□

Exercise 0.7. 4.3 - 49

Proof. First, notice that for any integer z, either z or $z+1$ is divisible by 2: Euclid's algorithm shows that for any z, we may write $z = 2y + r$ for some integer y and $r = 0$ or $r = 1$. If $r = 0$, then z is even. If $r = 1$, then $z + 1 = 2y + 2$, which is clearly divisible by 2.

Secondly, for any integer z, one of z, $z+1$ or $z+2$ is divisible by 3. Given z, by Euclid's algorithm, we may find an integer y and some $r \in \{0, 1, 2\}$ so that $z = 3y + r$. If $r = 0$, z is divisible by 3. If $r = 1$, then $z + 2 = 3y + 3$, which is divisible by 3. If $r = 2$, then $z + 1 = 3y + 3$ which is divisible by 3.

It follows that for any z both 2 and 3 divide $z(z+1)(z+2)$. Hence 6 divides $z(z+1)(z+2)$. □

Exercise 0.8. 4.3 - 52

Proof. False: $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 59 \cdot 503$, and is therefore not prime. □

Exercise 0.9. 4.4 - 2

Proof. We have to show 937 is an inverse of 13 mod 2436. This is just a calculation: we compute $937 \times 13 = 12,181$ and then we want to check that 2436 divides $12,181 - 1 = 12,180$. But an easy long division gives $12,181$ divided by 2436 is 5 which completes the argument. □

Exercise 0.10. 4.4 - 6(b).

Proof. First, we run Euclid's algorithm. We get

$$\begin{aligned} 89 &= 2 \cdot 34 + 21 \\ 34 &= 21 + 13 \\ 21 &= 13 + 8 \\ 13 &= 8 + 5 \\ 8 &= 5 + 3 \\ 5 &= 3 + 2 \\ 3 &= 2 + 1. \end{aligned}$$

Solving for the remainder and working backwards, we get

$$\begin{aligned} 1 = 3 - 2 &= 3 - (5 - 3) \\ &= 2 \cdot 3 - 5 \\ &= 2 \cdot (8 - 5) - 5 \\ &= 2 \cdot 8 - 3 \cdot 5 \\ &= 2 \cdot 8 - 3 \cdot (13 - 8) \\ &= 5 \cdot 8 - 3 \cdot 13 \\ &= 5 \cdot (21 - 13) - 3 \cdot 13 \\ &= 5 \cdot 21 - 8 \cdot 13 \\ &= 5 \cdot 21 - 8 \cdot (34 - 21) \\ &= 13 \cdot 21 - 8 \cdot 34 \\ &= 13 \cdot (89 - 2 \cdot 34) - 8 \cdot 34 \\ &= 13 \cdot 89 - 34 \cdot 34. \end{aligned}$$

So an inverse for 34 modulo 89 is -34, or $89 - 34 = 55$. □

Exercise 0.11. 4.4 - 6(c)

Proof. First, we run Euclid's algorithm:

$$\begin{aligned} 233 &= 144 + 89 \\ 144 &= 89 + 55 \\ 89 &= 55 + 34 \\ 55 &= 34 + 21 \\ 34 &= 21 + 13 \\ 21 &= 13 + 8 \\ 13 &= 8 + 5 \\ 13 &= 8 + 5 \\ 8 &= 5 + 3 \\ 5 &= 3 + 2 \\ 3 &= 2 + 1. \end{aligned}$$

Solving for the remainder in each of the above equations and then substituting, we get the following by working up from the bottom:

$$\begin{aligned} 1 = 3 - 2 &= 3 - (5 - 3) \\ &= 2 \cdot 3 - 5 \\ &= 2 \cdot (8 - 5) - 5 \\ &= 2 \cdot 8 - 3 \cdot 5 \\ &= 2 \cdot 8 - 3 \cdot (13 - 8) \\ &= 5 \cdot 8 - 3 \cdot 13 \\ &= 5 \cdot (21 - 13) - 3 \cdot 13 \\ &= 5 \cdot 21 - 8 \cdot 13 \\ &= 5 \cdot 21 - 8(34 - 21) \\ &= 13 \cdot 21 - 8 \cdot 34 \\ &= 13(55 - 34) - 8 \cdot 34 \\ &= 13 \cdot 55 - 21 \cdot 34 \\ &= 13 \cdot 55 - 21 \cdot (89 - 55) \\ &= 13 \cdot 55 - 21 \cdot 89 \\ &= 34 \cdot 55 - 21 \cdot 89 \\ &= 34 \cdot (144 - 89) - 21 \cdot 89 \\ &= 34 \cdot 144 - 55 \cdot 89 \\ &= 34 \cdot 144 - 55 \cdot (233 - 144) \\ &= 89 \cdot 144 - 55 \cdot 233. \end{aligned}$$

In conclusion, we get the equation $1 = 89 \cdot 144 - 55 \cdot 233$, which implies $89 \cdot 144 \equiv 1 \mod 233$. So 89 is a multiplicative inverse of 144 modulo 233. □

Exercise 0.12. 4.4 - 7

Proof. Suppose $ax \equiv 1 \mod m$ and $bx \equiv 1 \mod m$. Then $xb \equiv 1 \mod m$ which implies $axb \equiv a \mod m$, but as $ax \equiv 1 \mod m$ means that we have $axb \equiv b \mod m$. Hence $a \equiv b \mod m$. □

Exercise 0.13. 4.4 - 12(b)

Proof. In problem 6(c), we showed that the inverse of 144 mod 233 is 89. So to solve $144x \equiv 4 \mod 233$, we have

$$89 \cdot 144x \equiv 1x \equiv x \equiv 89 \cdot 4 \mod 233.$$

so $x \equiv 276 \mod 233$ so $x = 276$ or $x = 43$ works. □

Exercise 0.14. 4.4 - 12(c)

Proof. We have $1001 = 5 \cdot 200 + 1$ so $1001 - 5 \cdot 200 = 1$ which shows that -5 is an inverse to 200. To solve $200x \equiv 13 \mod 1001$ we compute $-5 \cdot 13 = -65$ so we have

$$x \equiv -5 \cdot 200 \equiv -5 \cdot 13 \equiv -65 \equiv 936 \mod 1001.$$

□

Exercise 0.15. 4.4 - 16

Proof. (a) We have the following identities

$$\begin{aligned} 2 \cdot 6 = 12 &\equiv 1 \mod 11 \\ 3 \cdot 4 = 12 &\equiv 12 \mod 11 \\ 7 \cdot 8 = 56 &\equiv 1 \mod 11 \\ 5 \cdot 9 = 45 &\equiv 1 \mod 11 \end{aligned}$$

This establishes (a).

(b) Notice that by reordering the product, we have

$$10! = (2 \cdot 6)(3 \cdot 4)(7 \cdot 8)(5 \cdot 9) \cdot 10 \equiv 10 \mod 11.$$

As $10 \equiv -1 \mod 11$, this shows $10! \equiv -1 \mod 11$. □

Exercise 0.16. 4.4 - 17

Proof. Suppose $x^2 \equiv 1 \mod p$. Then $p|x^2 - 1$. We may factor $x^2 - 1 = (x+1)(x-1)$. Then $p|(x+1)$ or $p|(x-1)$. This shows $x \equiv 1 \mod p$ or $x \equiv -1 \mod p$. □

Exercise 0.17. 4.4 - 20

Proof. We want to find all solutions to the system of congruences $x \equiv 2 \mod 3$, $x \equiv 1 \mod 4$, $x \equiv 3 \mod 5$. Define numbers m_1, m_2, m_3 by

$$\begin{aligned} m_1 &= \frac{3 \cdot 4 \cdot 5}{3} = 20 \\ m_2 &= = \frac{3 \cdot 4 \cdot 5}{4} = 15 \\ m_3 &= \frac{3 \cdot 4 \cdot 5}{5} = 12. \end{aligned}$$

We want to solve the congruences

$$\begin{aligned} m_1 y &\equiv 2 \mod 3 \\ m_2 z &\equiv 1 \mod 4 \\ m_3 w &\equiv 3 \mod 5. \end{aligned}$$

We can solve this using Euclid's algorithm to find multiplicative inverses for m_i, but in this case it is easy enough to do it by hand: $y = 1$ works as $20 \equiv 2 \mod 3$. We can set $z = 3$ as $45 \equiv 1 \mod 4$, and we can put $w = 4$ as $48 \equiv 3 \mod 5$. Then we can set

$$x = 1 \cdot 20 + 3 \cdot 15 + 4 \cdot 12 = 113.$$

This solution is congruent to $53 \mod 60$. By the Chinese Remainder theorem, there is a unique solution to this system of congruences mod 60, which means that any solution is of the form $x = 53 + 60z$ for some integer z. □

Exercise 0.18. 4.4 - 29

Proof. We argue that if $m_1, \ldots, m_n$ are relatively prime then if $m_i|a - b$ then $m_1 m_2 \ldots m_n | a - b$. First, note that an integer x divides an integer y if and only if every prime occuring in the prime factorization of x also occurs in the prime factorization of y with exponent greater than or equal to the exponent it has in the prime factorization of x. As the m_is are relatively prime, they share no prime factor in common. Hence if p is a prime occuring in the prime factorization of $m_1 \ldots m_n$, then there is a unique i so that $p|m_i$. Then as $m_i|a - b$, the exponent of p in the prime factorization of $a - b$ is greater than or equal to the exponent of p in the prime factorization of m_i, hence in $m_1 \ldots m_n$. This shows $m_1 \ldots m_n | a - b$.

It follows immediately from the definition that if $a \equiv b \mod m_i$ for all i, then $a \equiv b \mod m_1 m_2 \ldots m_n$. □

Exercise 0.19. 4.4 - 30

Proof. If x and y are two solutions to a system of linear congruences satisfying the hypotheses of the Chinese Remainder Theorem, then $x \equiv y \mod m_i$ for $i = 1, \ldots, n$. By the previous exercise, this shows $x \equiv y \mod m_1 \ldots m_n$. This shows that a solution is unique mod $m_1 \ldots m_n$. □

Exercise 0.20. 4.4 - 38

Proof. Fermat's little theorem shows that $5|3^4 - 1$, $7|3^6 - 1$ and $11|3^{10} - 1$. It follows that $3^4 \equiv 1 \mod 5$, $3^6 \equiv 1 \mod 7$ and $3^{10} \equiv 1 \mod 11$. Now we may compute

$$\begin{aligned} 3^{302} &= 3^{300} \cdot 3^2 = (3^4)^{75} \cdot 3^2 \equiv (1)^{75} \cdot 9 \equiv 4 \mod 5 \\ 3^{302} &= 3^{300} \cdot 3^2 = (3^6)^{50} \cdot 3^2 \equiv (1)^{50} \cdot 3^2 \equiv 9 \equiv 2 \mod 7 \\ 3^{302} &= 3^{300} \cdot 3^2 = (3^{10})^{30} \cdot 3^2 \equiv (1)^{30} \cdot 9 \equiv 9 \mod 11. \end{aligned}$$

□