VE203 Discrete Math

Spring 2022 — Worksheet 6 Solutions

April 16, 2022

Exercise 6.1 Modular Arithmetic

Find each of these values.

a) $(-133 \bmod 23 + 261 \bmod 23) \bmod 23$

b) $(457 \bmod 23 \cdot 182 \bmod 23) \bmod 23$

Solution:

a) Working modulo 23 , we have $-133 + 261 = 128 \equiv 13$, so the answer is 13 .

b) Working modulo 23 , we have $457 \cdot 182 \equiv 20 \cdot 21 = 420 \equiv 6$.

Exercise 6.2 Fermat's (Little) Theorem

Show that $2^{11,213} - 1$ is not divisible by 11 .

Solution:

By Fermat's theorem, $2^{10} \equiv 1(\bmod 11)$, so

$$\begin{aligned} 2^{11,213} - 1 &\equiv \left[\left(2^{10}\right)^{1,121} \cdot 2^3\right] - 1 \equiv \left[1^{1,121} \cdot 2^3\right] - 1 \\ &\equiv 2^3 - 1 \equiv 8 - 1 \equiv 7(\bmod 11) \end{aligned}$$

Exercise 6.3 Euler's Theorem

1. Compute $\varphi\left(p^2\right)$ where p is a prime.
2. Compute $\varphi(pq)$ where both p and q are primes.

Solution:

1. All positive integers less than p^2 that are not divisible by p are relatively prime to p. Thus welete from the $p^2 - 1$ integers less than p^2 the integers $p, 2p, 3p, \cdots, (p-1)p$. There are $p - 1$ integers deleted, so $\phi\left(p^2\right) = \left(p^2 - 1\right) - (p - 1) = p^2 - p$

2. We delete from the $pq - 1$ integers less than pq those that are mltiples of p or of q to obtain those relatively prime to pq. The multiples of p are $p, 2p, 3p, \cdots, (q-1)p$ and the multiples of q are $q, 2q, 3q, \cdots, (p-1)q$. Thus we delete a total of $(q-1)+(p-1) = p+q-2$ elements, so $\phi(pq) = (pq - 1) - (p + q + 2) = pq - p - q + 1 = (p - 1)(q - 1)$.

Exercise 6.4 Congruences

Find all solutions of the congruence $12x \equiv 27(\bmod 18)$.

Solution:

The gcd of 12 and 18 is 6 , and 6 is not a divisor of 27. Thus by the preceding theorem, there are no solutions.

Exercise 6.5 Solving Congruences

What are the solutions of the linear congruence $101x \equiv 583(\bmod 4620)$?

Solution:

1. The gcd of 101 and 4620 is 1 , and 1 is a divisor of 583. Thus by the preceding theorem, there is a solution.

2. Find an inverse of 101 modulo 4620.

The steps used by the Euclidean algorithm to find gcd(101, 4620) are

$$\begin{aligned}
4620 &= 45 \cdot 101 + 75 \\
101 &= 1 \cdot 75 + 26 \\
75 &= 2 \cdot 26 + 23 \\
26 &= 1 \cdot 23 + 3 \\
23 &= 7 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
2 &= 2 \cdot 1
\end{aligned}$$

3. Because the last nonzero remainder is 1 , we know that $\gcd(101, 4620) = 1$. We can now express $\gcd(101, 4620) = 1$ in terms of each successive pair of remainders.

In each step we eliminate the remainder by expressing it as a linear combination of the divisor and the dividend. We obtain

$$\begin{aligned}
1 &= 3 - 1 \cdot 2 \\
&= 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3 \\
&= -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23 \\
&= 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = -9 \cdot 75 + 26 \cdot 26 \\
&= -9 \cdot 75 + 26 \cdot (101 - 1 \cdot 75) = 26 \cdot 101 - 35 \cdot 75 \\
&= 26 \cdot 101 - 35 \cdot (4620 - 45 \cdot 101) = -35 \cdot 4620 + 1601 \cdot 101
\end{aligned}$$

4. 1601 is an inverse of 101 modulo 4620.

5. Multiplying both sides of the congruence by 1601 shows that $1601 \cdot 101x \equiv 1601 \cdot 583(\bmod 4620)$ Because $161701 \equiv 1(\bmod 4620)$ and $933383 \equiv 143(\bmod 4620)$, it follows that if x is a solution, then $x \equiv 143(\bmod 4620)$.

Exercise 6.6 Fast Modular Exponentiation

$$2^{2021} \bmod 2021$$

Solution:

Consider $2^{2021} \bmod 2021$. We first note that the binary representation of 2021 is

$$2021 = 2^{10} + 2^9 + 2^8 + 2^7 + 2^6 + 2^5 + 2^2 + 2^0.$$

Then we know that $2^{2021} = 2^{2^{10}+2^9+2^8+2^7+2^6+2^5+2^2+2^0} = 2^{2^{10}} \times 2^{2^9} \times 2^{2^8} \times 2^{2^7} \times 2^{2^6} \times 2^{2^5} \times 2^{2^2} \times 2^{2^0}$

Calculating that

$$\begin{aligned}
2^1 &\equiv 2 \bmod 2021 \\
2^{2^2} &\equiv 16 \bmod 2021 \\
2^{2^5} &\equiv 747 \bmod 2021 \\
2^{2^6} &\equiv 213 \bmod 2021 \\
2^{2^7} &\equiv 907 \bmod 2021 \\
2^{2^8} &\equiv 102 \bmod 2021 \\
2^{2^9} &\equiv 299 \bmod 2021 \\
2^{2^{10}} &\equiv 477 \bmod 2021
\end{aligned}$$

$$2^{2021} \equiv 477 \times 299 \times 102 \times 907 \times 213 \times 747 \times 16 \times 2 \equiv 1322 \bmod 2021$$

Exercise 6.7 Chinese Remainder Theorem

Solve the following system of linear congruence

$$\begin{aligned} x &\equiv 6 \pmod{11} \\ x &\equiv 13 \pmod{16} \\ x &\equiv 9 \pmod{21} \\ x &\equiv 19 \pmod{25} \end{aligned}$$

Solution:

Solution: Since $11, 16, 21,$ and 25 are pairwise relatively prime, the Chinese Remainder Theorem tells us that there is a unique solution modulo m, where $m = 11{\cdot}16{\cdot}21{\cdot}25 = 92400$.

We apply the technique of the Chinese Remainder Theorem with

$$k = 4, \quad m_1 = 11, \quad m_2 = 16, \quad m_3 = 21, \quad m_4 = 25,$$

$$a_1 = 6, \quad a_2 = 13, \quad a_3 = 9, \quad a_4 = 19,$$

to obtain the solution.

We compute

$$\begin{aligned} z_1 &= m/m_1 = m_2m_3m_4 = 16 \cdot 21 \cdot 25 = 8400 \\ z_2 &= m/m_2 = m_1m_3m_4 = 11 \cdot 21 \cdot 25 = 5775 \\ z_3 &= m/m_3 = m_1m_2m_4 = 11 \cdot 16 \cdot 25 = 4400 \\ z_4 &= m/m_4 = m_1m_3m_3 = 11 \cdot 16 \cdot 21 = 3696 \\ y_1 &\equiv z_1^{-1} (\bmod m_1) \equiv 8400^{-1} (\bmod 11) \equiv 7^{-1} (\bmod 11) \equiv 8 (\bmod 11) \\ y_2 &\equiv z_2^{-1} (\bmod m_2) \equiv 5775^{-1} (\bmod 16) \equiv 15^{-1} (\bmod 16) \equiv 15 (\bmod 16) \\ y_3 &\equiv z_3^{-1} (\bmod m_3) \equiv 4400^{-1} (\bmod 21) \equiv 11^{-1} (\bmod 21) \equiv 2 (\bmod 21) \\ y_4 &\equiv z_4^{-1} (\bmod m_4) \equiv 3696^{-1} (\bmod 25) \equiv 21^{-1} (\bmod 25) \equiv 6 (\bmod 25) \\ w_1 &\equiv y_1z_1 (\bmod m) \equiv 8 \cdot 8400 (\bmod 92400) \equiv 67200 (\bmod 92400) \\ w_2 &\equiv y_2z_2 (\bmod m) \equiv 15 \cdot 5775 (\bmod 92400) \equiv 86625 (\bmod 92400) \\ w_3 &\equiv y_3z_3 (\bmod m) \equiv 2 \cdot 4400 (\bmod 92400) \equiv 8800 (\bmod 92400) \\ w_4 &\equiv y_4z_4 (\bmod m) \equiv 6 \cdot 3696 (\bmod 92400) \equiv 22176 (\bmod 92400) \end{aligned}$$

The solution, which is unique modulo 92400 , is

$$\begin{aligned} x &\equiv a_1w_1 + a_2w_2 + a_3w_3 + a_4w_4 (\bmod 92400) \\ &\equiv 6 \cdot 67200 + 13 \cdot 86625 + 9 \cdot 8800 + 19 \cdot 22176 (\bmod 92400) \\ &\equiv 2029869 (\bmod 92400) \\ &\equiv \mathbf{89469} (\bmod 92400) \end{aligned}$$

Exercise 6.8 RSA

In an RSA procedure, the public key is chosen as $(n, E) = (2077, 97)$, i.e., the encryption function e is given by

$$e(x) = x^{97} \pmod{2077}$$

(Note that $2077 = 31 \times 67$.)

Compute the private key D, where $D = E^{-1}(\bmod \varphi(n))$. Decrypt the message 279 , that is, find x if $y = e(x) = 279(\bmod 2077)$.

Solution:

Note that $\varphi(2077) = (31-1)(67-1) = 1980$. We need to solve $97D \equiv 1 \pmod{1980}$. By Euclidean algorithm (or anything else that works)

$$\begin{aligned}
1980 &= 97 \times 20 + 40 \\
97 &= 40 \times 2 + 17 \\
40 &= 17 \times 2 + 6 \\
17 &= 6 \times 2 + 5 \\
6 &= 5 \times 1 + 1
\end{aligned}$$

hence

$$\begin{aligned}
1 &= 6 - 5 \\
&= 6 - (17 - 6 \times 2) = 6 \times 3 - 17 \\
&= (40 - 17 \times 2) \times 3 - 17 = 40 \times 3 - 17 \times 7 \\
&= 40 \times 3 - (97 - 40 \times 2) \times 7 = 40 \times 17 - 97 \times 7 \\
&= (1980 - 97 \times 20) \times 17 - 97 \times 7 \\
&= 1980 \times 17 - 97 \times 347
\end{aligned}$$

Thus $D \equiv -347 \equiv 1633 (\mathrm{mod} 1980)$.

We need to calculate $279^D (\mathrm{mod} 2077)$. First note that

$$1633 = (11001100001)_2 = 2^{10} + 2^9 + 2^6 + 2^5 + 2^0$$

Then

$$\begin{aligned}
279^{2^0} &\equiv 279 \quad (\mathrm{mod} 2077) \\
279^{2^1} &\equiv 279^2 \equiv 992 \quad (\mathrm{mod} 2077) \\
279^{2^2} &\equiv 992^2 \equiv -434 \quad (\mathrm{mod} 2077) \\
279^{2^3} &\equiv (-434)^2 \equiv -651 \quad (\mathrm{mod} 2077) \\
279^{2^4} &\equiv (1426)^2 \equiv 93 \quad (\mathrm{mod} 2077) \\
279^{2^5} &\equiv 93^2 \equiv 341 \quad (\mathrm{mod} 2077) \\
279^{2^6} &\equiv 341^2 \equiv (-31) \quad (\mathrm{mod} 2077) \\
279^{2^7} &\equiv (-31)^2 \equiv 961 \quad (\mathrm{mod} 2077) \\
279^{2^8} &\equiv 961^2 \equiv 1333 \quad (\mathrm{mod} 2077) \\
279^{2^9} &\equiv 1333^2 \equiv 1054 \quad (\mathrm{mod} 2077) \\
279^{2^{10}} &\equiv 1054^2 \equiv -279 \quad (\mathrm{mod} 2077)
\end{aligned}$$

$$\begin{aligned}
279^{1633} &\equiv 279^{2^0} + 2^5 + 2^6 + 2^9 + 2^{10} \\
&\equiv 279^{2^0} \cdot 279^{2^5} \cdot 279^{2^6} \cdot 279^{2^9} \cdot 279^{2^{10}} \\
&\equiv (279)(341)(-31)(1054)(-279) \\
&\equiv (-403)(-31)(1054)(-279) \\
&\equiv (31)(1054)(-279) \\
&\equiv (-558)(-279) \\
&\equiv 1984 \quad (\mathrm{mod} 2077)
\end{aligned}$$

Reference

1. Rosen, Kenneth H., and Kamala Krithivasan. Discrete mathematics and its applications: with combinatorics and graph theory. Tata McGraw-Hill Education, 2012.