

Math 1137, Summer 2003

Homework 8: 2,4,7,19,21,22,36,37 p.179; 2,5,6,12,27a),28a) p.194

Exercise: 2 p.179

a) 321:

$$\begin{aligned}321 &= 2 \times 160 + 1 \\160 &= 2 \times 80 + 0 \\80 &= 2 \times 40 + 0 \\40 &= 2 \times 20 + 0 \\20 &= 2 \times 10 + 0 \\10 &= 2 \times 5 + 0 \\5 &= 2 \times 2 + 1 \\2 &= 2 \times 1 + 0 \\1 &= 2 \times 0 + 1\end{aligned}$$

The upshot of the following sequence of integer divisions is that $321 = (101000001)_2$

b) 1023: For this problem, we can use a shortcut. To use the shortcut, you need to notice that $1023 = 2^{10} - 1$. (As a comparison, think of like $10^4 - 1 = 9,999$.) We have:

$$1023 = (1000000000)_2 - (1)_2 = (111111111)_2$$

c) 100632: For this integer, let's use an alternate approach to the one presented in class (and used in part a). We will start from the top and each time try to fit in the largest power of two we can:

$$\begin{aligned}100632 &= 2^{16} + 35096 \\&= 2^{16} + 2^{15} + 2328 \\&= 2^{16} + 2^{15} + 2^{11} + 280 \\&= 2^{16} + 2^{15} + 2^{11} + 2^8 + 24 \\&= 2^{16} + 2^{15} + 2^{11} + 2^8 + 2^4 + 8 \\100632 &= 2^{16} + 2^{15} + 2^{11} + 2^8 + 2^4 + 2^3\end{aligned}$$

Thus $100632 = (11000100010001000)_2$.

Exercise: 4 p.179

a) $(11011)_2 = 2^4 + 2^3 + 0 \times 2^2 + 2 + 1 = 27$.

b) $(1010110101)_2 = 2^9 + 2^7 + 2^5 + 2^4 + 2^2 + 1 = 693$.

c) $(1110111110)_2 = 2^9 + 2^8 + 2^7 + 2^5 + 2^4 + 2^3 + 2^2 + 2^1 = 958$.

d) $11111000011111_2 = 2^{14} + 2^{13} + 2^{12} + 2^{11} + 2^{10} + 2^4 + 2^3 + 2^2 + 2^1 + 1 = 31775$

Exercise: 7 p.180

This exercise asks us to write $(ABCDEF)_{16}$ in binary form. This is actually easier than it might seem because $16 = 2^4$. Thus every hexadecimal digit corresponds to a block of four bits. For example, $A_{16} = 10_{10} = (1010)_2$. Doing the same thing with the other hexadecimal digits and grouping them in blocks of four, we deduce that:

$$(ABCDEF)_{16} = (1010101110011011101111)_2$$

Exercise: 19 p.180

We want to find $3^{2003} \pmod{99}$. We do this by taking successive powers of 3 and at each time taking the remainder

modulo 99. We will find a pattern at some point and then it will be come clear what the answer is.

$$\begin{aligned}3 &\equiv 3 \pmod{99} \\3^2 &\equiv 9 \pmod{99} \\3^3 &\equiv 27 \pmod{99} \\3^4 &\equiv 81 \pmod{99} \\3^5 &\equiv 3 \times 81 \equiv 243 \equiv 45 \pmod{99} \\3^6 &\equiv 3 \times 45 \equiv 135 \equiv 36 \pmod{99} \\3^7 &\equiv 3 \times 36 \equiv 108 \equiv 9 \pmod{99}\end{aligned}$$

We can stop here because we now know that the pattern of remainders between the 9's will repeat. Hence, we can conclude that for $n \geq 2$ we have

$$3^n \equiv \begin{cases} 9 & \text{if } n \equiv 2 \pmod{5} \\ 27 & \text{if } n \equiv 3 \pmod{5} \\ 81 & \text{if } n \equiv 4 \pmod{5} \\ 45 & \text{if } n \equiv 0 \pmod{5} \\ 36 & \text{if } n \equiv 1 \pmod{5} \end{cases}$$

Since $2003 \equiv 3 \pmod{5}$, we can conclude that $3^{2003} \pmod{99} = 27$. (By the way, 3^{2003} has 955 digits.)

Exercise: 21 p.180

In all of the integer divisions here below, we will write $n = qd + r$.

a) $\gcd(18, 12) = 6$ because by Euclidean Algorithm

$$\begin{aligned}18 &= 1 \times 12 + 6 \\12 &= 2 \times 6 + 0\end{aligned}$$

b) $\gcd(111, 201) = 3$ because:

$$\begin{aligned}201 &= 1 \times 111 + 90 \\111 &= 1 \times 90 + 21 \\90 &= 4 \times 21 + 6 \\21 &= 3 \times 6 + 3 \\6 &= 2 \times 3 + 0\end{aligned}$$

c) $\gcd(1001, 1331) = 11$ because:

$$\begin{aligned}1331 &= 1 \times 1001 + 330 \\1001 &= 3 \times 330 + 11 \\330 &= 33 \times 11 + 0\end{aligned}$$

d) $\gcd(12345, 54321) = 3$ because:

$$\begin{aligned}54321 &= 4 \times 12345 + 4941 \\12345 &= 2 \times 4941 + 2463 \\4941 &= 2 \times 2463 + 15 \\2463 &= 164 \times 15 + 3 \\15 &= 5 \times 3 + 0\end{aligned}$$

e) $\gcd(1000, 5040) = 40$ because:

$$\begin{aligned}5040 &= 5 \times 1000 + 40 \\1000 &= 25 \times 40 + 0\end{aligned}$$

f) $\gcd(9888, 6060) = 12$ because:

$$\begin{aligned}9888 &= 1 \times 6060 + 3828 \\6060 &= 1 \times 3828 + 2232 \\3828 &= 1 \times 2232 + 1596 \\2232 &= 1 \times 1596 + 636 \\1596 &= 2 \times 636 + 324 \\636 &= 1 \times 324 + 312 \\324 &= 1 \times 312 + 12 \\312 &= 26 \times 12 + 0\end{aligned}$$

Exercise: 22 p.180

a) $\gcd(5, 1) = 1$ because by Euclidean Algorithm

$$5 = 5 \times 1 + 0$$

b) $\gcd(101, 100) = 1$ because:

$$\begin{aligned}101 &= 1 \times 100 + 1 \\100 &= 100 \times 1 + 0\end{aligned}$$

c) $\gcd(277, 123) = 1$ because:

$$\begin{aligned}277 &= 2 \times 123 + 311 \\123 &= 3 \times 31 + 30 \\31 &= 1 \times 30 + 1 \\30 &= 30 \times 1 + 0\end{aligned}$$

d) $\gcd(14039, 1529) = 139$ because:

$$\begin{aligned}14039 &= 9 \times 1529 + 278 \\1529 &= 5 \times 278 + 139 \\278 &= 2 \times 139 + 0\end{aligned}$$

e) $\gcd(14038, 1529) = 1$ because:

$$\begin{aligned}14038 &= 9 \times 1529 + 277 \\1529 &= 5 \times 277 + 144 \\277 &= 1 \times 144 + 133 \\144 &= 1 \times 133 + 11 \\133 &= 12 \times 11 + 1 \\11 &= 11 \times 1 + 0\end{aligned}$$

f) $\gcd(111111, 11111) = 1$ because:

$$\begin{aligned}111111 &= 10 \times 11111 + 1 \\11111 &= 11111 \times 1 + 0\end{aligned}$$

Exercise: 36 p.181

I know that other texts explain two's complement in a very simple way. However, I will follow the explanations of the text to get the two's complement expressions of various numbers. In this problem, we use, bitstrings of length $n = 6$ so we are considering integers x that lie in the range $-2^5 \leq x \leq 2^5 - 1$, i.e in the range $-32 \leq x \leq 31$.

- a) 22 is positive, so the two's complement starts with a 0 and the remaining bits simply represent the number 22 in usual binary. Two's complement of 22 is 010110.
- b) Same reasoning for 31. Two's complement is 011111.
- c) $x = -7$. In Two's complement, the first bit is now a 1 since x is negative. By the procedure, the remaining bits are the binary expansion of $2^{n-1} - |x| = 32 - 7 = 25$. Two's complement of -7: 111001.
- d) $x = -19$. $2^{n-1} - |x| = 13$. Two's complement of -19: 101101.

Exercise: 37 p.181

In these exercises, $n = 5$ so $2^{n-1} = 16$.

- a) $1001_2 = 9$ so in Two's complement $11001 = -(16 - 9) = -7$.
- b) $1101_2 = 13$ so in Two's complement $01101 = 13$.
- c) $0001_2 = 1$ so in Two's complement $10001 = -(16 - 1) = -15$.
- d) $1111_2 = 15$ so in Two's complement $11111 = -(16 - 15) = -1$.

What makes two's complement quick to implement is that the method described in the text is equivalent the following. To pass from a number n to its negative in two's complement, do a bitwise NOT on the binary expression of n and then add 1.

Exercise: 2 p.194

- a) $\gcd(9, 11) = 1$. A linear combination of 9 and 11 that gives 1 is: $5 \times 11 - 6 \times 9 = 1$.
- b) $\gcd(33, 44) = 11$. A linear combination of 33 and 44 that gives 11 is: $1 \times 44 - 1 \times 33 = 11$.
- c) $\gcd(35, 78) = 1$. A linear combination of 35 and 78 that gives 1 is: $29 \times 35 - 13 \times 78 = 1$.
- d) $\gcd(21, 55) = 1$. A linear combination of 21 and 55 that gives 1 is: $-8 \times 55 + 21 \times 21 = 1$.
- e) $\gcd(101, 203) = 1$. A linear combination of 101 and 203 that gives 1 is: $1 \times 203 - \times 101 = 1$.
- f) $\gcd(124, 323) = 1$. A linear combination of 323 and 124 that gives 1 is: $43 \times 323 - 112 \times 124 = 1$.
- g) $\gcd(2002, 2339) = 1$. For these big ones, let's follow the method in the book given to calculate a linear combination that give the greatest common divisor. Start by doing the Euclidean Algorithm.

$$\begin{aligned}
 2339 &= 1 \times 2002 + 337 \\
 2002 &= 5 \times 337 + 317 \\
 337 &= 1 \times 317 + 20 \\
 317 &= 15 \times 20 + 17 \\
 20 &= 1 \times 17 + 3 \\
 17 &= 5 \times 3 + 2 \\
 3 &= 1 \times 2 + 1 \\
 2 &= 2 \times 1 + 0
 \end{aligned}$$

Starting with the second to last line and each time eliminating the smallest remainder by using the previous line, we have:

$$\begin{aligned}
 1 &= 3 - 1 \times 2 \\
 &= 3 - 1 \times (17 - 5 \times 3) = 6 \times 3 - 1 \times 17 \\
 &= 6 \times (20 - 1 \times 17) - 1 \times 17 = 6 \times 20 - 7 \times 17 \\
 &= 6 \times 20 - 7 \times (317 - 15 \times 20) = 111 \times 20 - 7 \times 317 \\
 &= 111 \times (337 - 317) - 7 \times 317 = 111 \times 337 - 118 \times 317 \\
 &= 111 \times 337 - 118 \times (2002 - 5 \times 337) = 701 \times 337 - 118 \times 2002 \\
 &= 701 \times (2339 - 2002) - 118 \times 2002 = 701 \times 2339 - 819 \times 2002
 \end{aligned}$$

h) $\gcd(4669, 3457) = 1$. Here's Euclidean Algorithm:

$$\begin{aligned}4669 &= 1 \times 3457 + 1212 \\3457 &= 2 \times 1212 + 1033 \\1212 &= 1 \times 1033 + 179 \\1033 &= 5 \times 179 + 138 \\179 &= 1 \times 138 + 41 \\138 &= 3 \times 41 + 15 \\41 &= 2 \times 15 + 11 \\15 &= 1 \times 11 + 4 \\11 &= 2 \times 4 + 3 \\4 &= 1 \times 3 + 1 \\3 &= 3 \times 1 + 0\end{aligned}$$

Following the same method as in the previous exercise (after a lot of writing on scratch paper) we get $1252 \times 3457 - 927 \times 4669$.

i) $\gcd(10001, 13422) = 1$. The linear combination that gives this is $1793 \times 10001 - 1336 \times 13422$.

Exercise: 5 p.194

We want to find an inverse to 4 modulo 9. This is essential guessing and checking (though there are a few methods that get us there).

$$\begin{aligned}2 \times 4 &= 8 \equiv 8 \pmod{9} \\3 \times 4 &= 12 \equiv 3 \pmod{9} \\4 \times 4 &= 16 \equiv 7 \pmod{9} \\5 \times 4 &= 20 \equiv 2 \pmod{9} \\6 \times 4 &= 24 \equiv 6 \pmod{9} \\7 \times 4 &= 28 \equiv 1 \pmod{9}\end{aligned}$$

We can stop now since we've found that 7 is the inverse to 4 modulo 9.

Exercise: 6 p.194

We want to find an inverse to 2 modulo 17. Here's an adhoc method that shows other ways we can use congruences. Notice that $17 = 2^4 + 1$ and hence $2^4 \equiv -1 \pmod{17}$. Squaring both sides, we get $2^8 \equiv 1 \pmod{17}$. Thus 2^7 serves as an inverse of 2 modulo 17 and $2^7 \pmod{17} = 9$. Thus 9 is an inverse to 2 modulo 17.

Exercise: 12 p.194

Using the result of exercise 6, it's now easy to solve the congruence equation $2x \equiv 7 \pmod{17}$. We multiply both sides of the equation by 9 and get:

$$\begin{aligned}9 \times 2x &\equiv 9 \times 7 \pmod{17} \\18x &\equiv 63 \pmod{17} \\x &\equiv 12 \pmod{17}\end{aligned}$$

Exercise: 27a p.195

Fermat's Little Theorem says that for any number a such that $p \nmid a$, we have $a^{p-1} \equiv 1 \pmod{p}$. Consequently, with $p = 11$ we have $a^{10} \equiv 1 \pmod{11}$ for all integers a not divisible by 11. Thus

$$2^{340} \equiv (2^{10})^{34} \equiv 1^{34} \equiv 1 \pmod{11}$$

Exercise: 28a p.195

The three situations the problem asks us to look at are with the primes 5, 7 and 11. In order to take advantage of Fermat's Little Theorem, we need to know the congruence of 302 modulo 4, 6 and 10.

$$302 \equiv 2 \pmod{4}$$

$$302 \equiv 2 \pmod{6}$$

$$302 \equiv 2 \pmod{10}$$

For $p = 5$, we have

$$3^{302} \equiv 3^{75 \times 4 + 2} \equiv (3^4)^{75} \times 3^2 \equiv 1 \times 9 \equiv 4 \pmod{5}$$

For $p = 7$, we have

$$3^{302} \equiv 3^{50 \times 6 + 2} \equiv (3^6)^{50} \times 3^2 \equiv 1 \times 9 \equiv 2 \pmod{7}$$

For $p = 11$, we have

$$3^{302} \equiv 3^{30 \times 10 + 2} \equiv (3^{10})^{30} \times 3^2 \equiv 1 \times 9 \equiv 9 \pmod{11}$$