Example 61. Every integer x is congruent to one of $0, 1, 2, 3, 4$ modulo 5.

We therefore say that $0, 1, 2, 3, 4$ form a **complete set of residues** modulo 5.

Another natural complete set of residues modulo 5 is: $0, \pm 1, \pm 2$

A not so natural complete set of residues modulo 5 is: $-5, 2, 9, -2, 6$

A possibly natural complete set of residues modulo 5 is: $0, 3, 3^2 = 9, 3^3 = 27, 3^4 = 81$

[We will talk more about this last case. Because we obtained a complete set of residues this way, we will say that "3 is a multiplicative generator modulo 5".]

Review. a is invertible modulo n if and only if $\gcd(a, n) = 1$. We can compute a^{-1} using the Euclidean algorithm.

Example 62. (review) Determine $16^{-1} \pmod{25}$.

Solution. Using the Euclidean algorithm, in Example 15, we found that $11 \cdot 16 - 7 \cdot 25 = 1$.
Reducing that modulo 25, we get $11 \cdot 16 \equiv 1 \pmod{25}$.
Hence, $16^{-1} \equiv 11 \pmod{25}$.

Example 63. List all invertible residues modulo 10.

Solution. $1, 3, 7, 9$ (or, possibly, more compact and transparent: $\pm 1, \pm 3$)
[We start with all residues $0, 1, 2, \ldots, 9$ and only keep those which are coprime to 10.]

5.2 Linear congruences

Let us consider the linear congruence $ax \equiv b \pmod{n}$ where we are looking for solutions x.

We will regard solutions x_1, x_2 as the same if $x_1 \equiv x_2 \pmod{n}$.

Example 64. (review) Solve $16x \equiv 4 \pmod{25}$.

Solution. We first find $16^{-1} \pmod{25}$. Bézout's identity: $-7 \cdot 25 + 11 \cdot 16$.
Reducing this modulo 25, we get $11 \cdot 16 \equiv 1 \pmod{25}$.
Hence, $16^{-1} \equiv 11 \pmod{25}$.
It follows that $16x \equiv 4 \pmod{25}$ has the (unique) solution $x \equiv 16^{-1} \cdot 4 \equiv 11 \cdot 4 \equiv 19 \pmod{25}$.

Example 65.

(a) $3x \equiv 2 \pmod{7}$ has the solution $x = 3$. We regard $x = 10$ or $x = 17$ as the same solution. We therefore write that $x \equiv 3 \pmod{7}$ is the unique solution to the equation.

(b) $3x \equiv 2 \pmod{9}$ has no solutions x.

Why? Reducing $3x = 2 + 9m$ modulo 3, we get $0 \equiv 2 \pmod{3}$ which is a contradiction.
Just to make sure! Why does the same argument not apply to $3x \equiv 2 \pmod{7}$?

(c) $6x \equiv 3 \pmod{9}$ has solutions $x = 2$, $x = 5$, $x = 8$.

$6x = 3 + 9m$ is equivalent to $2x = 1 + 3m$ or $2x \equiv 1 \pmod{3}$. Which has solution $x \equiv 2 \pmod{3}$.

Armin Straub
straub@southalabama.edu

Theorem 66. Consider the linear congruence $ax \equiv b \pmod{n}$. Let $d = \gcd(a, n)$.

(a) The linear congruence has a solution if and only if $d|b$.

(b) If $d = 1$, then there is a unique solution modulo n.

(c) If $d|b$, then it has d different solutions modulo n.

(In fact, it has a unique solution modulo n/d.)

Proof.

(a) Finding x such that $ax \equiv b \pmod{n}$ is equivalent to finding x, y such that $ax + ny = b$.
The latter is a diophantine equation of the kind we studied earlier. In particular, we know that it has a solution if and only if $\gcd(a, n)$ divides b.

(b) If $d = 1$, then a is invertible modulo n. Multiplying the congruence $ax \equiv b \pmod{n}$ with a^{-1}, we obtain $x \equiv a^{-1}b \pmod{n}$. That's the unique solution.
Alternatively. If $d = 1$, then $ax + ny = b$ has general solution $x = x_0 + tn$, $y = y_0 - ta$ (where x_0, y_0 is some particular solution). But, modulo n, all of these lead to the same solution $x \equiv x_0 \pmod{n}$.

(c) If $d|b$, then $ax \equiv b \pmod{n}$ is equivalent to $a_1 x \equiv b_1 \pmod{n_1}$ with $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$, $n_1 = \frac{n}{d}$. (Make sure you see why! Spell out the congruences as equalities.) Since $\gcd(a_1, n_1) = 1$, we get a unique solution x modulo n_1.
Being congruent to x modulo n_1 is the same as being congruent to one of $x, x + n_1, \ldots, x + (d-1)n_1$ modulo n. □

Example 67. Solve the system

$$\begin{aligned} 7x + 3y &\equiv 10 \pmod{16} \\ 2x + 5y &\equiv 9 \pmod{16}. \end{aligned}$$

Solution. As a first step we solve the system:

$$\begin{aligned} 7x + 3y &= 10 \\ 2x + 5y &= 9 \end{aligned}$$

However you prefer solving this system (two options below), you will find the unique solution $x = \frac{23}{29}$, $y = \frac{43}{29}$.
To obtain a solution to the congruences modulo 16, all we have to do is to determine $29^{-1} \pmod{16}$ and then use that to reinterpret the solution we just obtained.
$29^{-1} \equiv (-3)^{-1} \equiv 5 \pmod{16}$. Thus, $x = 29^{-1} \cdot 23 \equiv 5 \cdot 7 \equiv 3 \pmod{16}$ and $y = 29^{-1} \cdot 43 \equiv 5 \cdot 11 \equiv 7 \pmod{16}$.
Comment. We should check our answer: $7 \cdot 3 + 3 \cdot 7 = 42 \equiv 10 \pmod{16}$, $2 \cdot 3 + 5 \cdot 7 = 41 \equiv 9 \pmod{16}$.

A naive way to solve 2×2 systems. To solve $7x+3y=10$, $2x+5y=9$, we can use the second equation to write $x=\frac{9}{2}-\frac{5}{2}y$ and substitute that into the first equation: $7\left(\frac{9}{2}-\frac{5}{2}y\right)+3y=10$, which simplifies to $\frac{63}{2}-\frac{29}{2}y=10$. This yields $y=\frac{43}{29}$. Using that value in, say, the first equation, we get $7x+3\cdot\frac{43}{29}=10$, which results in $x=\frac{23}{29}$.

Solving 2×2 systems using matrix inverses. The equations $7x+3y=10$, $2x+5y=9$ can be expressed as

$$\begin{bmatrix} 7 & 3 \\ 2 & 5 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}=\begin{bmatrix} 10 \\ 9 \end{bmatrix},$$

assuming we are familiar with the basic matrix-vector calculus. A solution is then given by

$$\begin{bmatrix} x \\ y \end{bmatrix}=\begin{bmatrix} 7 & 3 \\ 2 & 5 \end{bmatrix}^{-1}\begin{bmatrix} 10 \\ 9 \end{bmatrix}=\frac{1}{35-6}\begin{bmatrix} 5 & -3 \\ -2 & 7 \end{bmatrix}\begin{bmatrix} 10 \\ 9 \end{bmatrix}=\frac{1}{29}\begin{bmatrix} 23 \\ 43 \end{bmatrix}.$$

Here, we used that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1}=\frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix},$$

one of the few formulas worth memorizing.

Advanced comment. It follows from the matrix inverse discussion that the system

$$\begin{aligned} ax+by &\equiv r \pmod n \\ cx+dy &\equiv s \pmod n \end{aligned}$$

has a unique solution modulo n if $\gcd(ad-bc,n)=1$.

The matrix $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ is invertible if and only if $ad-bc\neq 0$ (that is, $ad-bc$ is invertible).

The matrix $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ is invertible modulo n if and only if $\gcd(ad-bc,n)=1$ (that is, $ad-bc$ is invertible modulo n).

Comment. You can also see Theorem 4.9 and Example 4.11 in our textbook for a direct approach modulo 16.

Example 68. (extra) Solve the system

$$\begin{aligned} 2x-y &\equiv 7 \pmod{15} \\ 3x+4y &\equiv -2 \pmod{15}. \end{aligned}$$

Solution. As a first step we solve the system:

$$\begin{aligned} 2x-y &= 7 \\ 3x+4y &= -2 \end{aligned}$$

You can solve the system any way you like. For instance, using a matrix inverse, we find

$$\begin{bmatrix} x \\ y \end{bmatrix}=\begin{bmatrix} 2 & -1 \\ 3 & 4 \end{bmatrix}^{-1}\begin{bmatrix} 7 \\ -2 \end{bmatrix}=\frac{1}{11}\begin{bmatrix} 4 & 1 \\ -3 & 2 \end{bmatrix}\begin{bmatrix} 7 \\ -2 \end{bmatrix}=\frac{1}{11}\begin{bmatrix} 26 \\ -25 \end{bmatrix}.$$

To obtain a solution to the congruences modulo 15, we determine that $11^{-1}\equiv -4 \pmod{15}$ (you might be able to see this modular inverse; in any case, practice using the Euclidean algorithm to compute these).

Therefore, $x=11^{-1}\cdot 26\equiv -4\cdot 11\equiv 1 \pmod{15}$ and $y=11^{-1}\cdot(-25)\equiv -4\cdot 5\equiv 10 \pmod{15}$.

Check our answer. $2\cdot 1-10=-8\equiv 7 \pmod{15}$, $3\cdot 1+4\cdot 10=43\equiv -2 \pmod{15}$.

6 Fermat's little theorem

Example 69. (warmup) What a terrible blunder... Explain what is wrong!

$$\text{(incorrect!)} \quad 10^9 \equiv 3^2 = 9 \equiv 2 \pmod 7$$

Solution. $10^9 = 10 \cdot 10 \cdot \ldots \cdot 10 \equiv 3 \cdot 3 \cdot \ldots \cdot 3 = 3^9$. Hence, $10^9 \equiv 3^9 \pmod 7$.

However, there is no reason, why we should be allowed to reduce the exponent by 7 (and it is incorrect).

Corrected calculation. $3^2 \equiv 2$, $3^4 \equiv 4$, $3^8 \equiv 16 \equiv 2$. Hence, $3^9 = 3^8 \cdot 3^1 \equiv 2 \cdot 3 \equiv -1 \pmod 7$.

By the way, this approach of computing powers via exponents that are $2,\ 4,\ 8,\ 16,\ 32,\ \ldots$ is called **binary exponentiation**. It is crucial for efficiently computing large powers (see below).

Corrected calculation (using Fermat). $3^6 \equiv 1 \pmod 7$ just like $3^0 = 1$. Hence, we are allowed to reduce exponents modulo 6. Consequently, $3^9 \equiv 3^3 \equiv -1 \pmod 7$.

Theorem 70. (Fermat's little theorem) Let p be a prime, and suppose that $p \nmid a$. Then

$$a^{p-1} \equiv 1 \pmod p.$$

Proof. The first $p-1$ multiples of a, namely

$$a, 2a, 3a, \ldots, (p-1)a,$$

are all different modulo p. (Why?!!) Clearly, none of them is divisible by p.

Consequently, the values form a complete set of residues with the residue 0 missing. In other words, these values are congruent (in some order) to the values $1, 2, \ldots, p-1$ modulo p. Thus,

$$a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod p.$$

Cancelling the common factors (allowed because p is prime!), we get $a^{p-1} \equiv 1 \pmod p$. □

Remark. The "little" in this theorem's name is to distinguish this result from Fermat's last theorem that $x^n + y^n = z^n$ has no integer solutions if $n > 2$ (only recently proved by Wiles).

Comment. An alternative proof based on induction is given in our book (bottom of page 88).

Example 71. What is 2^{100} modulo 3? That is, what is the remainder upon division by 3?

Solution. $2 \equiv -1 \pmod 3$. Hence, $2^{100} \equiv (-1)^{100} = 1 \pmod 3$.

Careful! Once more, it is incorrect to reduce the exponent modulo 3! $100 \equiv 1 \pmod 3$ but $2^{100} \not\equiv 2^1 \pmod 3$.

Comment. However, since we are working modulo a prime, $p = 3$, Fermat's little theorem does allow us to reduce the exponent modulo $p - 1 = 2$. Indeed, $2^{100} \equiv 2^0 \equiv 1 \pmod 3$.

Example 72. Compute $3^{1003} \pmod{101}$.

Solution. Since 101 is a prime, $3^{100} \equiv 1 \pmod{101}$ by Fermat's little theorem.

Therefore, $3^{1003} = 3^{10 \cdot 100} \cdot 3^3 \equiv 3^3 = 27 \pmod{101}$.

Important comment. Note that, because of Fermat's little theorem, we can reduce the exponent modulo 100 when calculating modulo 101. In particular, since $1003 \equiv 3 \pmod{100}$, we have $3^{1003} \equiv 3^3 = 27 \pmod{101}$.

7 Binary exponentiation

Example 73. Compute $3^{32} \pmod{101}$.

Solution. Fermat's little theorem is not helpful here.

$3^2 = 9$, $3^4 = 81 \equiv -20$, $3^8 \equiv (-20)^2 = 400 \equiv -4$, $3^{16} \equiv (-4)^2 \equiv 16$, $3^{32} \equiv 16^2 \equiv 54$, all modulo 101

Armin Straub
straub@southalabama.edu

Example 74. Compute $3^{25} \pmod{101}$.

Solution. Fermat's little theorem is not helpful here.
Instead, we do what is called **binary exponentiation**:
$3^2 = 9$, $3^4 = 81 \equiv -20$, $3^8 \equiv (-20)^2 = 400 \equiv -4$, $3^{16} \equiv (-4)^2 \equiv 16$, all modulo 101
Since $25 = 16 + 8 + 1$, we have $3^{25} = 3^{16} \cdot 3^8 \cdot 3^1 \equiv 16 \cdot (-4) \cdot 3 = -192 \equiv 10 \pmod{101}$.

Every integer $n \geqslant 0$ can be written as a sum of distinct powers of 2 (in a unique way). Therefore our approach to compute powers always works. It is called **binary exponentiation**.
Because $25 = \boxed{1} \cdot 2^4 + \boxed{1} \cdot 2^3 + \boxed{0} \cdot 2^2 + \boxed{0} \cdot 2^1 + \boxed{1} \cdot 2^0$, we will write $25 = (11001)_2$.

Example 75. Compute $407^{37249} \pmod{101}$.

Solution. First, $407^{37249} \equiv 3^{37249} \pmod{101}$. Then, using Fermat, $3^{37249} \equiv 3^{49} \pmod{101}$.
We then use binary exponentiation:
$3^2 = 9$, $3^4 = 81 \equiv -20$, $3^8 \equiv (-20)^2 = 400 \equiv -4$, $3^{16} \equiv (-4)^2 \equiv 16$, $3^{32} \equiv 16^2 \equiv 54$, all modulo 101
Since $49 = (110001)_2 = 2^0 + 2^4 + 2^5$, we have $3^{49} = 3^{32} \cdot 3^{16} \cdot 3^1 \equiv 54 \cdot 16 \cdot 3 \equiv 67 \pmod{101}$.
In conclusion, $407^{37249} \equiv 67 \pmod{101}$.

Example 76. (extra) Using binary exponentiation, compute $5^{49} \pmod{105}$.

Solution. Recall that $49 = (110001)_2 = 2^0 + 2^4 + 2^5$.
$5^1 = 5$, $5^2 = 25$, $5^4 = 25^2 = 625 \equiv -5$, $5^8 \equiv (-5)^2 = 25$, $5^{16} \equiv 25^2 \equiv -5$, $5^{32} \equiv (-5)^2 = 25$
Hence, $5^{49} = 5^{32} \cdot 5^{16} \cdot 5^1 \equiv 25 \cdot (-5) \cdot 5 \equiv 5$.

8 Representations of integers in different bases

Example 77. We are commonly using the **decimal system** of writing numbers:

$$1234 = 4 \cdot 10^0 + 3 \cdot 10^1 + 2 \cdot 10^2 + 1 \cdot 10^3.$$

10 is called the base, and $1, 2, 3, 4$ are the digits in base 10. To emphasize that we are using base 10, we will write $1234 = (1234)_{10}$. Likewise, we write

$$(1234)_b = 4 \cdot b^0 + 3 \cdot b^1 + 2 \cdot b^2 + 1 \cdot b^3.$$

In this example, $b > 4$, because, if b is the base, then the digits have to be in $\{0, 1, \ldots, b-1\}$.

Important note. If the least significant digit of x in base b is x_0, then $x \equiv x_0 \pmod{b}$.

Example 78. Express 25 in base 2.

Solution. We already noticed that $25 = 16 + 8 + 1 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$. Hence, $25 = (11001)_2$.
Alternatively, here's how we could have determined the digits without prior knowledge:

- $25 = 12 \cdot 2 + \boxed{1}$. Hence, $25 = (\ldots 1)_2$ where $\ldots$ are the digits for 12.
- $12 = 6 \cdot 2 + \boxed{0}$. Hence, $25 = (\ldots 01)_2$ where $\ldots$ are the digits for 6.
- $6 = 3 \cdot 2 + \boxed{0}$. Hence, $25 = (\ldots 001)_2$ where $\ldots$ are the digits for 3.
- $3 = 1 \cdot 2 + \boxed{1}$, with $\boxed{1}$ left over. Hence, $25 = (11001)_2$.

Example 79. Express 49 in base 2.

Solution.

- $49 = 24 \cdot 2 + \boxed{1}$. Hence, $49 = (\ldots 1)_2$ where $\ldots$ are the digits for 24.
- $24 = 12 \cdot 2 + \boxed{0}$. Hence, $49 = (\ldots 01)_2$ where $\ldots$ are the digits for 12.
- $12 = 6 \cdot 2 + \boxed{0}$. Hence, $49 = (\ldots 001)_2$ where $\ldots$ are the digits for 6.
- $6 = 3 \cdot 2 + \boxed{0}$. Hence, $49 = (\ldots 0001)_2$ where $\ldots$ are the digits for 3.
- $3 = 1 \cdot 2 + \boxed{1}$, with $\boxed{1}$ left over. Hence, $49 = (110001)_2$.

Other bases. What is 49 in base 3? $49 = 16 \cdot 3 + \boxed{1}$, $16 = 5 \cdot 3 + \boxed{1}$, $5 = 1 \cdot 3 + \boxed{2}$, $\boxed{1}$. Hence, $49 = (1211)_3$.
What is 49 in base 7? $49 = (100)_7$.

Review. Fermat's little theorem, expressing numbers in different bases

Example 80. (review) Express 31 in base 2.

Solution. $31 = (11111)_2$

There is nothing special about the base 10 that we are used to (except that we have 10 fingers).

In fact, since 10 is not a prime, base 10 is not particularly nice mathematically.

Example 81. Add $(1210)_3$ and $(1121)_3$, working only in base 3.

Solution. We add with carries
$$\begin{array}{cccccc} & & 1 & 2 & 1 & 0 \\ + & & 1 & 1 & 2 & 1 \\ \hline & 1 & 0 & 1 & 0 & 1 \end{array}$$
and find that $(1210)_3 + (1121)_3 = (10101)_3$.

For comparison. $(1210)_3 = 3 + 2\cdot 9 + 27 = 48$, $(1121)_3 = 1 + 2\cdot 3 + 9 + 27 = 43$ and $(10101)_3 = 1 + 9 + 81 = 91$.

Review long multiplication from school! Then notice how it is easiest in base 2:

Example 82. Multiply $(110100)_2$ and $(101)_2$, working only in base 2.

Solution.
$$\begin{array}{cccccccccc} & & & & 1 & 1 & 0 & 1 & 0 & 0 \\ \times & & & & & & & 1 & 0 & 1 \\ \hline & & & & 1 & 1 & 0 & 1 & 0 & 0 \\ + & & 1 & 1 & 0 & 1 & 0 & 0 & & \\ \hline & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{array}$$
so that $(110100)_2 \cdot (101)_2 = (100000100)_2$.

For comparison. $(110100)_2 = 4 + 16 + 32 = 52$, $(101)_2 = 1 + 4 = 5$ and $(100000100)_2 = 4 + 256 = 260$.

Example 83. (divisibility by 9) A number $n = (a_m a_{m-1} \cdots a_0)_{10}$ is divisible by 9 if and only if the sum of its decimal digits $a_m + a_{m-1} + \ldots + a_0$ is divisible by 9.

Why? Note that $10^r \equiv 1^r \equiv 1 \pmod 9$ for any integer $r \geqslant 0$.

In particular, $n = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \ldots + a_1 \cdot 10^1 + a_0 \equiv a_m + a_{m-1} + \ldots + a_1 + a_0 \pmod 9$.

For instance. 1234567 is not divisible by 9 because $1+2+3+4+5+6+7 = 28$ is not divisible by 9. In fact, $1234567 \equiv 28 \equiv 10 \equiv 1 \pmod 9$.

Example 84. (divisibility by 11) A number $n = (a_m a_{m-1} \cdots a_0)_{10}$ is divisible by 11 if and only if the alternating sum of its decimal digits $(-1)^m a_m + (-1)^{m-1} a_{m-1} + \ldots + a_0$ is divisible by 11.

Why? Note that $10^r \equiv (-1)^r \pmod{11}$ for any integer $r \geqslant 0$. In particular,

$n = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \ldots + a_1 \cdot 10^1 + a_0 \equiv (-1)^m a_m + (-1)^{m-1} a_{m-1} + \ldots - a_1 + a_0 \pmod{11}$.

For instance. 123456 is not divisible by 11 because $6 - 5 + 4 - 3 + 2 - 1 = 3$ is not divisible by 11. In fact, $123456 \equiv 3 \pmod{11}$.

Example 85. Bases 2, 8 and 16 (binary, octal and hexadecimal) are commonly used in computer applications.

For instance, in JavaScript or Python, 0b... means $(\ldots)_2$, 0o... means $(\ldots)_8$, and 0x... means $(\ldots)_{16}$.

The digits $0, 1, \ldots, 15$ in hexadecimal are typically written as $0, 1, \ldots, 9, A, B, C, D, E, F$.

Problem. Which number is 0xD1?

Solution. 0xD1$= 13 \cdot 16 + 1 = 209$.

The South Alabama Jaguar NCAA team color code is 0xD11241. That means $\mathrm{RGB}(209, 18, 65)$, where each value (ranging from 0 to 255) quantifies the amount of red (R), green (G) and blue (B).

For instance, 0x000000 is black, and 0xFF0000 is red, and 0xFFFFFF is white.

We can thus see that the color 0xD11241 is close to a red (though not a pure one).

Armin Straub
straub@southalabama.edu

Example 86. How can we can compute the inverse of a modulo p via Fermat's little theorem?

Solution. By Fermat's little theorem, $a^{p-1} \equiv 1 \pmod{p}$.
Write $a^{p-1} = a \cdot a^{p-2}$ to see that it follows that $a^{-1} \equiv a^{p-2} \pmod{p}$.

For instance. Suppose we would like to compute $2^{-1} \pmod{7}$.
Since $2^6 \equiv 1 \pmod{7}$, by little Fermat, we conclude that $2^{-1} \equiv 2^5 = 32 \equiv 4 \pmod{7}$.

Comment. A similar approach (based on Euler's theorem, which we will discuss shortly) would work for computing inverses modulo composite numbers n. However, in that case, we essentially need to know the prime factorization of n, which is impractical for large n.

Example 87. (advanced) We can also express negative (or, even, rational) numbers in different bases. The following is a glimpse at p-adic analysis.

(a) **(again; review)** Express 31 in base 2.

(b) Express -1 in base 2.

(c) Express $1/3$ in base 2.

Solution.

(a) Note that $31 \equiv 1 \pmod{2}$, so that the least significant digit of $x = 31$ in base 2 must be 1.
The other digits then describe $(x-1)/2 = 15$.
In other words, $31 = (\ldots 1)_2$ where $\ldots$ are the digits for 15.
Continuing like this, we find $31 = (11111)_2$.

(b) Note that $-1 \equiv 1 \pmod{2}$, so that the least significant digit of $x = -1$ in base 2 must be 1.
The other digits then describe $(x-1)/2 = -1$.
In other words, $-1 = (\ldots 1)_2$ where $\ldots$ are the digits for -1.
We conclude that $-1 = (\ldots 1111)_2$, an infinite string of 1's.
Note. $x = -1$ is characterized by $x + 1 = 0$. Think about starting with $(\ldots 1111)_2$ and adding 1. Observe how we repeatedly get carries so that the result is indeed $(\ldots 0000)_2$.

(c) We proceed in the same fashion (and interpret fractions modulo 2 using modular inverses):

- Note that $1/3 \equiv 1 \pmod{2}$, so that the least significant digit of $x_1 = 1/3$ in base 2 must be 1.
  Hence, $1/3 = (\ldots 1)_2$ where $\ldots$ are the digits for $x_2 = (x_1 - 1)/2 = -1/3$.
- $-1/3 \equiv 1 \pmod{2}$, so that the next digit is 1.
  Hence, $1/3 = (\ldots 11)_2$ where $\ldots$ are the digits for $x_3 = (x_2 - 1)/2 = -2/3$.
- $-2/3 \equiv 0 \pmod{2}$, so that the next digit is 0.
  Hence, $1/3 = (\ldots 011)_2$ where $\ldots$ are the digits for $x_4 = (x_3 - 0)/2 = -1/3$.
- But we have seen $-1/3$ before! Everything will repeat from now on.
  We conclude that $1/3 = (\ldots 01010101011)_2$.

Note. $x = 1/3$ is characterized by $3x = 1$. Think about starting with $(\ldots 01010101011)_2$ and multiplying with $3 = (11)_2$. Can you see that the result is indeed 1?

$$\begin{array}{cccccccccc} & \ldots & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ \times & & & & & & & & 1 & 1 \\ \hline & \ldots & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ + & \ldots & 0 & 1 & 0 & 1 & 0 & 1 & 1 & \\ \hline & \ldots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}$$

Example. Russian multiplication!