Sketch of Lecture 10 Thu, 9/19/2019

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

Example 81. (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 82. 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 83. 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 84. (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 85. (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 86. Bases 2, 8 and 16 (binary, octal and hexadecimal) are commonly used in computer applications.

For instance, in JavaScript or Python, $0\text{b}\ldots$ means $(\ldots)_2$, $0\text{o}\ldots$ means $(\ldots)_8$, and $0\text{x}\ldots$ 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. $0\text{xD1} = 13 \cdot 16 + 1 = 209$.

The South Alabama Jaguar NCAA team color code is 0xD11241. That means $\text{RGB}(209, 18, 65)$, 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).

Example 87. 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 88. (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 ... 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 ... 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 ... 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 ... 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 ... 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?

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