basic course info

Class meetings Thu 6:30 - 9:20 in Olsen 408

Instructor Prof. Tibor Beke
Office Southwick 350P
E-mail `Tibor_Beke@uml.edu`
Office Hours (tentative) MW 13:30-15:00

Textbook
Klain: Essentials of Number Theory
Santos: Number Theory for Mathematical Contests

Posted on Blackboard (together with all slides and handouts).

what is number theory?

The study of the positive integers $1, 2, 3, \ldots$ under the operations of addition, multiplication and exponentiation. (This is sometimes called *elementary number theory*.)

Analytic number theory brings in the tools of calculus (real and complex analysis) to study properties of the distribution of primes and related questions.

Algebraic number theory lies at the intersection of abstract algebra and number theory. It studies *algebraic numbers* like expressions of the form $n + m\sqrt{2}$ where n, m are integers. Many properties of the usual integers, such as divisibility and primes, can be extended to rings of algebraic integers, but the picture becomes beautifully complicated.

teaser: divisibility test for 3 and 9

If the sum of the digits of a number is divisible by 3, then the number is divisible by 3.

teaser: divisibility test for 3 and 9

If the sum of the digits of a number is divisible by 3, then the number is divisible by 3.

Example: 111 is divisible by 3.

teaser: divisibility test for 3 and 9

If the sum of the digits of a number is divisible by 3, then the number is divisible by 3.

Example: 111 is divisible by 3.

Question: Is this true for negative integers?

teaser: divisibility test for 3 and 9

If the sum of the digits of a number is divisible by 3, then the number is divisible by 3.

Example: 111 is divisible by 3.

Question: Is this true for negative integers? Yes.

teaser: divisibility test for 3 and 9

If the sum of the digits of a number is divisible by 3, then the number is divisible by 3.

Example: 111 is divisible by 3.

Question: Is this true for negative integers? Yes.

If the sum of the digits of a number is divisible by 9, then the number is divisible by 9.

teaser: divisibility test for 3 and 9

If the sum of the digits of a number is divisible by 3, then the number is divisible by 3.

Example: 111 is divisible by 3.

Question: Is this true for negative integers? Yes.

If the sum of the digits of a number is divisible by 9, then the number is divisible by 9.

More generally, the sum of the digits of a number has the same remainder when divided by 9 as the number itself.

- Take a positive integer, e.g. 3,278,534.
- $3 + 2 + 7 + 8 + 5 + 3 + 4 = 32 = 3 \cdot 9 + 5$
- $3,278,534 - 5$ is divisible by 9.

teaser: divisibility test for 11

The *alternating* sum of the digits of a number has the same remainder when divided by 11 as the number itself.

- Take a positive integer, e.g. 278,534.
- $-2+7-8+5-3+4=3$
- $278534-3$ is divisible by 11.

- Take 1,718,534
- $1-7+1-8+5-3+4=-7$
- $1718534-(-7)$ is divisible by 11.

teaser: gcd times lcm

Take any two positive integers, say, 120 and 252.
Their greatest common divisor is 12.
Their least common multiple is 2520.

$$120 \cdot 252 = 12 \cdot 2520 = 30240$$

Is this a coincidence or what?

teaser: last digits

1 8 27 64 125 216 343 512 729 1000

teaser: last digits

1   8   27   64   125   216   343   512   729   1000

These are the first ten *cubes*. Their last digits go

$$1, 8, 7, 4, 5, 6, 3, 2, 9, 0$$

Each of $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ shows up exactly once as the last digit.

teaser: last digits

1 16 81 256 625 1296 2401 4096 6561 10000

teaser: last digits

1 16 81 256 625 1296 2401 4096 6561 10000

These are the first ten fourth powers. Their last digits go

$$1, 6, 1, 6, 5, 6, 1, 6, 1, 0$$

1 shows up 4 times, in locations 1,3,7,9.
6 shows up 4 times, in locations 2,4,6,8.
5 and 0 each show up once.

teaser: last digits

$$1 \quad 16 \quad 81 \quad 256 \quad 625 \quad 1296 \quad 2401 \quad 4096 \quad 6561 \quad 10000$$

These are the first ten fourth powers. Their last digits go

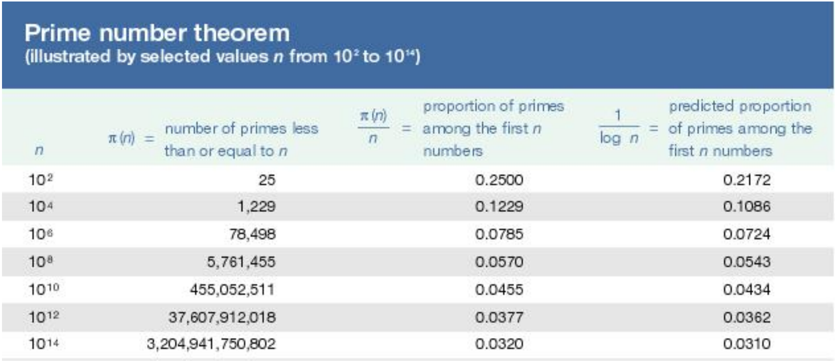
$$1, 6, 1, 6, 5, 6, 1, 6, 1, 0$$

1 shows up 4 times, in locations 1,3,7,9.
6 shows up 4 times, in locations 2,4,6,8.
5 and 0 each show up once.

The numbers $1, 3, 7, 9$ are exactly the numbers less than 10 that are *coprime* with 10. (That is, they have no integer divisors in common with 10.)

Is this a one-off, or part of a pattern? What sort of pattern?

teaser: the prime number theorem



Prime number theorem

(illustrated by selected values *n* from 10^2 to 10^{14})

n	$\pi(n)$ = number of primes less than or equal to *n*	$\frac{\pi(n)}{n}$ = proportion of primes among the first *n* numbers	$\frac{1}{\log\ n}$ = predicted proportion of primes among the first *n* numbers
10^2	25	0.2500	0.2172
10^4	1,229	0.1229	0.1086
10^6	78,498	0.0785	0.0724
10^8	5,761,455	0.0570	0.0543
10^{10}	455,052,511	0.0455	0.0434
10^{12}	37,607,912,018	0.0377	0.0362
10^{14}	3,204,941,750,802	0.0320	0.0310

$$\frac{\pi(n)}{n} \sim \frac{1}{\ln n}$$

where $\pi(n)$ is the number of prime numbers less than or equal to n.

tentative syllabus

- divisibility; modular arithmetic; divisibility tests; checksums
- gcd, lcm, Euclidean algorithm
- primes; unique factorization
- Chinese remainder theorem
- Euler's function and sums of divisors
- Fermat's, Wilson's and Lucas's theorems
- modular exponentiation and primitive roots
- quadratic residues; quadratic reciprocity

Final exam Take-home, due on the date set by the Registrar.
Will cover the entire semester, and accounts for 30% of your grade.

Midterm evaluation In class, Thu, Oct 10.
Will account for 20% of your grade.

Homework problems One set per week.
Accounts for 45% of your grade.

Class participation Accounts for 5% of your grade.
If you do not have unexcused absences, this 5% is automatic.

Email All official communication will be sent to your student email address, `Your_Name@student.uml.edu`.

Class attendance policy You are expected to be present at all class meetings and take all exams on their assigned dates. If you are unable to attend, notify me as soon as you can.

divisibility

$$\mathbb{N} := \{0, 1, 2, 3, \dots\}$$
$$\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$$

Our discussion of divisibility and modular arithmetic applies to all integers $\mathbb{Z}$, and it is in fact convenient *not to* restrict attention to the natural numbers $\mathbb{N}$.

Notation $d \mid n$ means that d divides n, that is, there exists an integer k such that $d \cdot k = n$.

$d \nmid n$ means that d does not divide n, that is, there is no integer k such that $d \cdot k = n$.

examples and basic properties

$17 \mid 51$

$19 \nmid 51$

examples and basic properties

$17 \mid 51$
$19 \nmid 51$

Is $17 \mid 0$ true?

examples and basic properties

$17 \mid 51$
$19 \nmid 51$

Is $17 \mid 0$ true? Yes.

examples and basic properties

$17 \mid 51$
$19 \nmid 51$

Is $17 \mid 0$ true? Yes.

Is $-17 \mid 51$ true?

examples and basic properties

$17 \mid 51$
$19 \nmid 51$

Is $17 \mid 0$ true? Yes.

Is $-17 \mid 51$ true? Yes.

examples and basic properties

$17 \mid 51$
$19 \nmid 51$

Is $17 \mid 0$ true? Yes.

Is $-17 \mid 51$ true? Yes.

- $d \mid 0$.
- If $a \mid b$ and $b \mid c$ then $a \mid c$.
- If $d \mid n$ and $n \neq 0$ then $|d| \leqslant |n|$.
- If $a \mid b$ and $b \mid a$ then $a = \pm b$.
- If $d \mid n$ and $d \mid m$ then $d \mid an + bm$ for all integers a, b.

division with remainder

Let n, d be integers, $d > 0$. Then there exist unique integers q, r such that $0 \leqslant r \leqslant d - 1$ and

$$n = q \cdot d + r$$

q is the (integer) quotient and r is the *remainder* when dividing n by d.

Indeed, $q = \lfloor \frac{n}{d} \rfloor$ and $r = n - qd$.

base d number systems

Fix an integer $d > 1$. Given an integer n, write it as $n = d \cdot n_0 + r_0$ with $0 \leqslant r_0 \leqslant d - 1$. Repeat this for n_0, i.e. let $n_0 = d \cdot n_1 + r_1$ with $0 \leqslant r_1 \leqslant d - 1$ and continue. Since $n > n_0 > n_1 > \dots$, the process terminates with $n_{k-1} = d \cdot 0 + r_k$ for some k. Putting it back together,

$$\begin{aligned} n &= d \cdot n_0 + r_0 \\ &= d(d \cdot n_1 + r_1) + r_0 \\ &= d(d \cdot (d \cdot n_2 + r_2) + r_1) + r_0 \\ &= \ \dots \\ &= d(d \cdot (d \cdot (\dots r_{k+1}) + \dots + r_2) + r_1) + r_0 \\ &= d^k \cdot r_k + d^{k-1} \cdot r_{k-1} + \dots + d^2 \cdot r_2 + d \cdot r_1 + r_0 \end{aligned}$$

base d number systems

A base d number representation

$$r_k \cdot d^k + r_{k-1} \cdot d^{k-1} + \cdots + r_2 \cdot d^2 + r_1 \cdot d + r_0$$

is usually abbreviated as

$$r_k r_{k-1} \ldots r_2 r_1 r_0 \,{}_d$$

examples

4356_{10} means $4 \cdot 10^3 + 3 \cdot 10^2 + 5 \cdot 10^1 + 6$
4356_7 means $4 \cdot 7^3 + 3 \cdot 7^2 + 5 \cdot 7^1 + 6$
1011001_2 means $2^6 + 2^4 + 2^3 + 2^0$

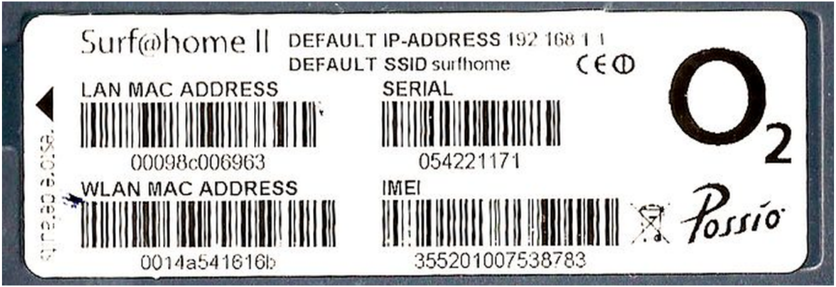
base d number systems

- *binary*: base 2. Digits (bits) are 0 and 1.
- *octal*: base 8. Digits are 0 through 7.
- *decimal*: our old friend, base 10.
- *hexadecimal*: base 16. “Digits” are 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F.

  A,B,C,D,E,F (also written in lower case) stand for 10,11,12,13,14,15 in turn.

Homework Problem 1

In the bottom left of this panel, you see an integer ("WLAN MAC ADDRESS") written in hexadecimal notion:



Surf@home II

DEFAULT IP-ADDRESS 192 168 1 1
DEFAULT SSID surfhome

LAN MAC ADDRESS
00098c006963

SERIAL
054221171

WLAN MAC ADDRESS
0014a541616b

IMEI
355201007538783

(Ignore the two initial 0's.) Write down this number in

- base 2
- base 8
- base 10.

Show your steps, not just the final answer!
Due Thu, Sept 12, in class.

division with remainder

$\{0, 1, 2, \ldots, d-1\}$ is not the only set of preferred remainders. There are many other choices; any set of d consecutive integers would do (and in fact, any set of representatives from the d remainder classes modulo d).

In practical applications, the most important alternative is the set of *balanced remainders*.

When d is even, these are

$$-\frac{d}{2}+1, -\frac{d}{2}+2, \ldots, -1, 0, 1, \ldots, \frac{d}{2}-1, \frac{d}{2}$$

When d is odd, these are

$$-\frac{d-1}{2}, -\frac{d-1}{2}+1, \ldots, -1, 0, 1, \ldots, \frac{d-1}{2}-1, \frac{d-1}{2}$$

division with remainder

Example

For $d = 6$, the balanced set of remainders is $\{-2, -1, 0, 1, 2, 3\}$.

For $d = 7$, it is $\{-3, -2, -1, 0, 1, 2, 3\}$.

$13 = 2 \cdot 6 + 1$

$10 = 2 \cdot 6 + (-2)$

$17 = 2 \cdot 7 + 3$

$18 = 3 \cdot 7 + (-3)$

base d number systems with other sets of “digits”

$\{0, 1, 2, \ldots, d-1\}$ is not the only complete set of remainders that can serve as digits.

Pick any $-d+2 \leqslant a \leqslant 0$ and consider $\{a, a+1, \ldots, a+d-1\}$. Can you use the *same* process to find the expansion of any positive integer n in the form

$$r_k \cdot d^k + r_{k-1} \cdot d^{k-1} + \cdots + r_2 \cdot d^2 + r_1 \cdot d + r_0$$

where $a \leqslant r_i \leqslant a+d-1$. The key is that the process terminates:

If $n = d \cdot n_0 + r_0$ then $n_0 < n$.

balanced ternary

Take the base $d = 3$ with digits $\{-1, 0, 1\}$.

Example

$$10(-1)(-1)010_3$$

means

$$1 \cdot 3^6 + 0 \cdot 3^5 + (-1) \cdot 3^4 + (-1) \cdot 3^3 + 0 \cdot 3^2 + 1 \cdot 3^1 + 0 \cdot 3^0$$

that is, $3^6 - 3^4 - 3^3 + 3 = 624$.

Upshot Any positive integer is expressible (uniquely!) as a sum of distinct powers of 3 with coefficients of $+1$ and -1.

This number system is called *balanced ternary* and has many fascinating properties.

Homework Problem 2

Express the number 2024 in base 5 using the “digits” -3,-2,-1,0,1 *only*.

Show your work, not just the final answer!

Due Thu, Sept 12, in class.

raising to power by repeated squaring

Let $\star$ be an associative operation on a set; that is,

$$(x \star y) \star z = x \star (y \star z)$$

Suppose you need to compute $x^{23} = x \star (x \star (x \star (\ldots (x \star x))..)$ (23 copies of 'x').

Could do this by 22 consecutive '$\star$' operations.

Or ...

raising to power by repeated squaring

compute $x^2 = x \star x$
compute $x^4 = x^2 \star x^2$
compute $x^8 = x^4 \star x^4$
compute $x^{16} = x^8 \star x^8$
compute $x^{20} = x^{16} \star x^4$
compute $x^{22} = x^{20} \star x^2$
compute $x^{23} = x^{22} \star x$

needing ‘$\star$’ operations.

raising to power by repeated squaring

compute $x^2 = x \star x$
compute $x^4 = x^2 \star x^2$
compute $x^8 = x^4 \star x^4$
compute $x^{16} = x^8 \star x^8$
compute $x^{20} = x^{16} \star x^4$
compute $x^{22} = x^{20} \star x^2$
compute $x^{23} = x^{22} \star x$

needing 7 '$\star$' operations.

application: raising to power by repeated squaring

Proposition

Suppose the positive integer k has a binary expansion that is n bits long and contains m 1's. Then it is possible to compute x^k using only $n+m-2$ multiplications.

Algorithm

$$k = b_{n-1}b_{n-2}\dots b_2b_1b_0 \quad \text{in base 2}$$

Compute x^2, $(x^2)^2 = x^4$, $(x^4)^2 = x^8$, $\dots$, $x^{2^{n-1}}$ in turn (that's $n-1$ consecutive squaring). Multiply $x^{2^{n-1}}$ by all the x^{2^i} with $b_i = 1$ for $0 \leqslant i < n-1$ (that's $m-1$ more multiplications). The product will be x^k.

Homework Problem 3

Which of the following statements are true?

(a) There are infinitely many positive integers n such that computing x^{n+1} by repeated squaring takes *more* multiplications than computing x^n by repeated squaring.

(b) There are infinitely many positive integers n such that computing x^{n+1} by repeated squaring takes *exactly as many* multiplications as computing x^n by repeated squaring.

(c) There are infinitely many positive integers n such that computing x^{n+1} by repeated squaring takes *fewer* multiplications than computing x^n by repeated squaring.

Justify your answer.

Due Thu, Sept 12, in class.

Homework Problem 4*

* This problem is optional. If you don't turn it in, it won't affect your grade. If you solve it correctly, you will receive bonus credit.

For $n \in \mathbb{N}$, let $M(n)$ denote the number of multiplications needed to compute x^n if you use the repeated squares algorithms.

What is the *average* number of multiplications needed to compute x^n for $1024 \leqslant n \leqslant 2047$? That is, find the value of

$$\frac{1}{1024}\Big(M(1024)+M(1025)+M(1026)+\cdots+M(2046)+M(2047)\Big)$$

Due (optionally) Thu, Sept 12, in class.

modular arithmetic: notation

Notation Writing

$$a \equiv b \pmod{n}$$

means that n divides $a - b$.

Same as saying that a and b have the same remainder (taken from some complete set of representatives) when divided by n.

One says that a and b are *congruent modulo n*.

$$1001 \equiv 1 \pmod{2}$$

$$51 \equiv 0 \pmod{3}$$

$$-17 \equiv 5 \pmod{11}$$

modular arithmetic: basic facts

- $a \equiv 0 \pmod{n}$ means $n \mid a$
- $a \equiv a \pmod{n}$
- if $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$
- if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$

If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$ then

$$a + b \equiv a' + b' \pmod{n}$$
$$a - b \equiv a' - b' \pmod{n}$$
$$ab \equiv a'b' \pmod{n}$$

If $a \equiv b \pmod{n}$ then $a^k \equiv b^k \pmod{n}$ for all positive integers k.

aside: another use for *mod n*

'mod n' is sometimes used as a function symbol, to denote taking the remainder of integer division by n. One usually means the remainder from the standard range $\{0, 1, 2, \ldots, n-1\}$.

Therefore

$$a \bmod n = b$$

means that the remainder of a when divided by n equals b.

$$\begin{aligned} 1001 \bmod 2 &= 1 \\ 51 \bmod 3 &= 0 \\ -17 \bmod 11 &= 5 \end{aligned}$$

modular arithmetic: fun

- What is the remainder of

$$73 \cdot 15^{65} + 69 \cdot 13^{101} - 30 \cdot 44 \cdot 38$$

when you divide it by 7?

Can you find the answer without a calculator?

modular arithmetic: fun

- What is the remainder of

$$73 \cdot 15^{65} + 69 \cdot 13^{101} - 30 \cdot 44 \cdot 38$$

when you divide it by 7?

Can you find the answer without a calculator?

- Show that

$$(3^{2024}-5)\cdot(3^{2024}-3)\cdot(3^{2024}-1)\cdot(3^{2024}+1)\cdot(3^{2024}+3)\cdot(3^{2024}+5)\cdot(3^{2024}+7)$$

is divisible by 7.

modular arithmetic: remainders from digits

What is the remainder of 46705 modulo 3?

$$46705 = 4 \cdot 10^4 + 6 \cdot 10^3 + 7 \cdot 10^2 + 0 \cdot 10^1 + 5$$

Since $10 \equiv 1 \pmod{3}$, it follows that $10^k \equiv 1^k = 1 \pmod{3}$
So the above number is congruent, modulo 3, to

$$4 + 6 + 7 + 0 + 5$$

the sum of its digits.

Same trick works modulo 9.

modular arithmetic: remainders from digits

$$10 \equiv -1 \bmod 11$$

$$10^k \equiv (-1)^k \bmod 11$$

therefore

$$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_k \cdot 10^k + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

is congruent modulo 11 to

$$a_n \cdot (-1)^n + a_{n-1} \cdot (-1)^{n-1} + \cdots + a_k \cdot (-1)^k + \cdots + a_2 \cdot (-1)^2 + a_1 \cdot (-1) + a_0$$

which is the sum of the digits with alternating +/- signs.
(The alternation is so that the rightmost digit, the "ones", get assigned '+')

$$(-1)^n \cdot a_n \cdots \pm \cdots - a_3 + a_2 - a_1 + a_0$$

Homework Problem 5

Go back to Homework Problem 1. You found a hexadecimal integer there (a number written in base 16 notation).

What is the remainder of that number when you divide it by 17?

Find out the answer using computations only with small integers.

Due Thu, Sept 12, in class.

modular arithmetic: remainders from consecutive digits

Is there a divisibility shortcut for the modulus 101?

$$41045678930$$

$$4|10|45|67|89|30$$

$$-4+10-45+67-89+30$$

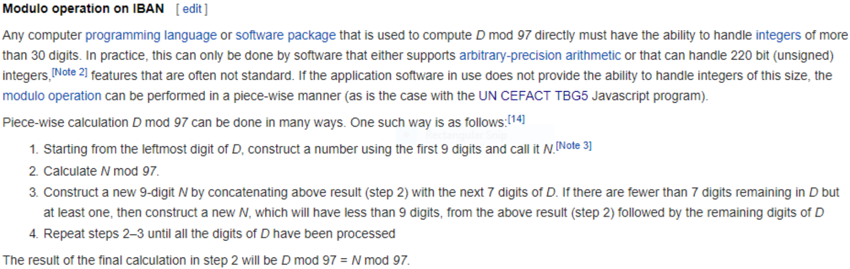
checksums

Long numerical codes (credit card numbers, bank routing numbers, ISBN identifiers etc) are almost never completely arbitrary, but are constructed so that the codes satisfy some number-theoretic condition. This allows software to check for potentially corrupted or invalid codes.

An example of such an identifier is the IBAN (International Bank Account Number). This is a *long* alphanumerical code that, after conversion into an integer, should be congruent to 1 modulo 97.

But how do you compute with 30-digit (or bigger) numbers, when most hardware does not allow calculations with integers having more than 64 bits? (Note: 2^{64} is about $2 \cdot 10^{19}$.)

A webpage gives the following recipe:



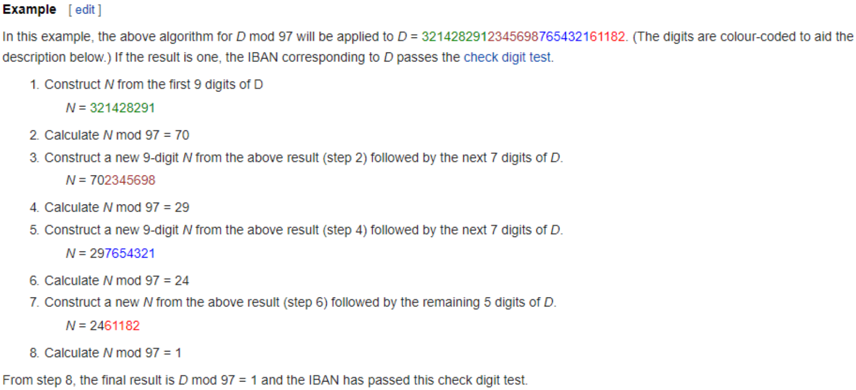
Modulo operation on IBAN [edit]

Any computer programming language or software package that is used to compute *D* mod *97* directly must have the ability to handle integers of more than 30 digits. In practice, this can only be done by software that either supports arbitrary-precision arithmetic or that can handle 220 bit (unsigned) integers,[Note 2] features that are often not standard. If the application software in use does not provide the ability to handle integers of this size, the modulo operation can be performed in a piece-wise manner (as is the case with the UN CEFACT TBG5 Javascript program).

Piece-wise calculation *D* mod *97* can be done in many ways. One such way is as follows:[14]

1. Starting from the leftmost digit of *D*, construct a number using the first 9 digits and call it *N*.[Note 3]
2. Calculate *N* mod *97*.
3. Construct a new 9-digit *N* by concatenating above result (step 2) with the next 7 digits of *D*. If there are fewer than 7 digits remaining in *D* but at least one, then construct a new *N*, which will have less than 9 digits, from the above result (step 2) followed by the remaining digits of *D*
4. Repeat steps 2–3 until all the digits of *D* have been processed

The result of the final calculation in step 2 will be *D* mod 97 = *N* mod *97*.



Example [edit]

In this example, the above algorithm for *D* mod 97 will be applied to *D* = 3214282912345698765432161182. (The digits are colour-coded to aid the description below.) If the result is one, the IBAN corresponding to *D* passes the check digit test.

1. Construct *N* from the first 9 digits of D

   N = 321428291

2. Calculate *N* mod 97 = 70
3. Construct a new 9-digit *N* from the above result (step 2) followed by the next 7 digits of *D*.

   N = 702345698

4. Calculate *N* mod 97 = 29
5. Construct a new 9-digit *N* from the above result (step 4) followed by the next 7 digits of *D*.

   N = 297654321

6. Calculate *N* mod 97 = 24
7. Construct a new *N* from the above result (step 6) followed by the remaining 5 digits of *D*.

   N = 2461182

8. Calculate *N* mod 97 = 1

From step 8, the final result is *D* mod 97 = 1 and the IBAN has passed this check digit test.

Homework Problem 6

Consider the 'remainder modulo 97' recipe found on the previous two slides.

- Is the recipe correct? Why?
- What is the special role played by 9? (Since the recipe calls for collecting *9* digits from the left.)

Due Thu, Sept 12, in class.

where we are in your textbooks

- divisibility: Klain section 4
- base d representations of integers: Klain section 5
- modular arithmetic, repeated squaring: beginning of Klain section 10
- divisibility tests: Klain section 12
- checksums: Klain section 13

In Santos, you can consult Chapters 2 and 3. The discussion there is much more compact and the problems much harder!