Number systems and the Chinese Remainder Theorem

(dedicated to Prof. Attila Pethő on occasion of his 60th birthday)

Christiaan van de Woestijne
Lehrstuhl für Mathematik und Statistik
Montanuniversität Leoben, Austria

Supported by the FWF, project S9610

Number theory and its applications
Debrecen, 4-8 October 2010

Number systems and pre-number systems

We define a pre-number system as a triple $(V, \phi, \mathcal{D})$, where

- V is an Abelian group;
- ϕ is an endomorphism of V of finite cokernel;
- $\mathcal{D}$ is a finite subset of V containing a system of representatives of V modulo $\phi(V)$.

A pre-number system $(V, \phi, \mathcal{D})$ is a number system if there exist finite expansions

$$a = \sum_{i=0}^{\ell} \phi^i(d_i) \qquad (d_i \in \mathcal{D})$$

for all $a \in V$.

We are ultimately interested in the classification of all number systems.

Examples

- $(\mathbb{Z}, b, \{0, \ldots, |b|-1\})$ is a pre-number system whenever $|b| \geq 2$, and a number system if and only if $b \leq -2$.
- $(\mathbb{Z}[i], b, \{0, \ldots, |b|^2-1\})$ is a pre-number system whenever $|b| > 1$, and a number system if and only if $b = -a \pm \mathrm{i}$, for some $a \in \mathbb{N}$.
- $(\mathbb{Z}[X]/((X-5)(X-7)), X, \{1, -1, 3, -3, 5, X, X-2, -X+2, X-4, -X+4, X-6, -X+6, X-8, -X+8, -X+10, 2X-7, 2X-9, -2X+9, 2X-11, -2X+11, 2X-13, -2X+13, -2X+15, 3X-14, 3X-16, -3X+16, -3X+18, 3X-18, -3X+20, 4X-21, 4X-23, -4X+23, -4X+25, 5X-28, -5X+30\})$ is a number system (proof: to come!).

Properties

If $(V, \phi, \mathcal{D})$ is a number system, then we call $\mathcal{D}$ a valid digit set for (V, ϕ).

If $\mathcal{D}$ contains elements that are congruent modulo $\phi(V)$, we call it redundant, otherwise irredundant.

Theorem (Okazaki/CvdW) If $(V, \phi, \mathcal{D})$ is a number system, then

$$V \cong V^{\text{tor}} \times H \text{ where } H \cong V/V^{\text{tor}}.$$

Also, H is a subgroup of a finite-dimensional $\mathbb{Q}$-vector space, so ϕ can be given by a finite-dimensional matrix over $\mathbb{Q}$.

Today, we consider V of the form $\mathbb{Z}[X]/(P)$, with $P \in \mathbb{Z}[X]$ non-constant, or closely related groups.

Note that when $(V, \phi, \mathcal{D})$ and $(W, \psi, \mathcal{E})$ are number systems, the direct product $(V \times W, \phi \times \psi, \mathcal{D} \times \mathcal{E})$ is well-defined and is also a number system.

Example: the odd digits

Assume $V = \mathbb{Z}$ and ϕ is multiplication by some integer b. Let b be odd, $|b| \geq 3$, and let

$$\mathcal{D}_{\text{odd}} := \{-|b|+2, -|b|+4, \ldots, -1, 1, \ldots, |b|-2, b\}.$$

This is a valid digit set for all odd b.

For $b = 3$: it's $\{-1, 1, 3\}$. We get $0 = 3 \cdot 1 + (-1) \cdot 3$.

a	$(a)_{3,\text{odd}}$	a	$(a)_{3,\text{odd}}$	a	$(a)_{3,\text{odd}}$	a	$(a)_{3,\text{odd}}$
0	$\overline{1}3$	5	$1\overline{1}\overline{1}$	-1	$\overline{1}$	-6	$\overline{1}133$
1	1	6	13	-2	$\overline{1}1$	-7	$\overline{1}1\overline{1}$
2	$1\overline{1}$	7	$1\overline{1}1$	-3	$\overline{1}13$	-8	$\overline{1}131$
3	3	8	$3\overline{1}$	-4	$\overline{1}\overline{1}$	-9	$\overline{1}\overline{1}3$
4	11	9	$1\overline{1}3$	-5	$\overline{1}11$	-10	$\overline{1}13\overline{1}$

Projections

Suppose f is a CNS polynomial, so

$$(\mathbb{Z}[X]/(f), X, \{0, \ldots, |f(0)| - 1\})$$

is a number system. If $f = f_1 f_2$, then trivially also

$$(\mathbb{Z}[X]/(f_i), X, \{0, \ldots, |f(0)| - 1\}) \quad (i = 1, 2)$$

are number systems (with possibly redundant digit sets): if

$$a = \sum_{i=0}^{\ell} d_i X^i \pmod{f},$$

then the same expansion is true modulo f_1 and f_2.

Can we go in the other direction? What is the relation with the direct product

$$\left(\frac{\mathbb{Z}[X]}{f_1}, X, \mathcal{D}_1\right) \times \left(\frac{\mathbb{Z}[X]}{f_2}, X, \mathcal{D}_2\right)?$$

The Chinese Remainder Theorem

Everybody knows this formulation: if $(n, m) = 1$, then

$$\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

How about this one: if $(f, g) = 1$, with $f, g \in \mathbb{Z}[X]$, then

$$\mathbb{Z}[X]/(fg) \cong \mathbb{Z}[X]/(f) \times \mathbb{Z}[X]/(g) \ ?$$

This is false in general! In $\mathbb{Q}[X]$ it works, because $\mathbb{Q}[X]$ is a PID, but $\mathbb{Z}[X]$ is not a PID. The correct statement is

$$\mathbb{Z}[X]/(fg) \cong \mathbb{Z}[X]/(f) \times_{\mathbb{Z}[X]/(f,g)} \mathbb{Z}[X]/(g),$$

where given maps $A, B \xrightarrow{\mu,\nu} C$, the fibred product $A \times_C B$ is defined as

$$\{(a, b) \in A \times B \mid \mu(a) = \nu(b)\}.$$

Really coprime polynomials

We have $\mathbb{Z}[X]/(fg) \cong \mathbb{Z}[X]/(f) \times_{\mathbb{Z}[X]/(f,g)} \mathbb{Z}[X]/(g)$.

Now suppose $(f, g) = (1)$; then $\mathbb{Z}[X]/(f, g)$ is the zero ring, so the fibred product is just the direct product. Recall that there exist $u, v \in \mathbb{Z}[X]$ with $uf + vg = \mathrm{Res}(f, g)$. Therefore:

Theorem Suppose $f, g \in \mathbb{Z}[X]$ have $\mathrm{Res}(f, g) = 1$. Then $(f, g) = (1)$. If the leading coefficients are coprime in $\mathbb{Z}$, then the converse holds, because we have $|\mathbb{Z}[X]/(f, g)| = |\mathrm{Res}(f, g)|$.

But (Myerson): let $f = 2X + 1$ and $g = 2X + (1 + 2^e)$ for some $e \geq 1$. Then $\mathrm{Res}(f, g) = 2^e$, but $(f, g) = (1)$.

In general, $\mathbb{Z}[X]/(f, g)$ has a complicated structure! Can be determined using strong Gröbner bases over $\mathbb{Z}$.

Conclusion (first try)

Theorem If $(\mathbb{Z}[X]/(f_i), X, \mathcal{D}_i)$, for $i = 1, 2$, are number systems, and $(f_1, f_2) = 1$, then

$$(\mathbb{Z}[X]/(f_1), X, \mathcal{D}_1) \times (\mathbb{Z}[X]/(f_2), X, \mathcal{D}_2) \cong (\mathbb{Z}[X]/(f_1 f_2), X, \mathcal{E})$$

with $\mathcal{E} = \mathcal{D}_1 \times \mathcal{D}_2$ via the CRT.

Of course, when we reduce $\mathcal{E}$ modulo f_i, we should get $\mathcal{D}_i$. So unfortunately we conclude that even when $\mathcal{D}_1$ and $\mathcal{D}_2$ are the canonical digits,

$$\mathcal{E} \neq \{0, 1, \ldots, |f_1(0) f_2(0) - 1|\}$$

(the canonical digits for $f_1 f_2$)!

Can we still make this into a nice birthday present for Attila?

Not really coprime polynomials

We still have $\mathbb{Z}[X]/(fg) \cong \mathbb{Z}[X]/(f) \times_{\mathbb{Z}[X]/(f,g)} \mathbb{Z}[X]/(g)$.

Try to extend this to number systems, so assume we have digits $\mathcal{D}_i$, and try to form digits modulo fg using the isomorphism.

It follows that $d \equiv d' \pmod{(f,g)}$ for all $d, d' \in \mathcal{D}_1 \cup \mathcal{D}_2$!!!

In particular, $\mathcal{D}_1$ and $\mathcal{D}_2$ cannot contain 0...

Let's try an example: $f = X - 3$, $g = X - 5$, so $(f,g) = (2)$ and

$$\mathbb{Z}[X]/(f,g) \cong \mathbb{Z}/2\mathbb{Z}.$$

It follows that all digits must be 1 modulo 2! But wait...

A worked example

We have the odd digits $\{-1, 1, 3\}$ for $X - 3$ and $\{-3, -1, 1, 3, 5\}$ for $X - 5$. Now use the Chinese Remainder Theorem, and get digits

$$\{1,\ -1,\ 3,\ -3,\ X,\ 3X - 10,\ -X + 4,\ 2X - 5,\ -3X + 12,\ X - 4,$$
$$-2X + 9,\ -X + 2,\ 2X - 7,\ -X + 6,\ X - 2,\ -2X + 7\}$$

for $(X - 3)(X - 5)$.

Using some more technical stuff, we will show that this digit set is valid.

Bad example: if we had digits 1 and 2, respectively, the isomorphism gives $\frac{1}{2}(X - 1)$, which is not integral, and this residue class is uniquely determined, by the CRT for $\mathbb{Q}[X]$.

Technical stuff

Following the map of reduction modulo (f, g), we obtain a number system in the finite ring $R = \mathbb{Z}[X]/(f, g)$; as we have seen, we assume there is just one digit d in this number system.

So all possible expansions are d, $d + dX$, $d + dX + dX^2$, ..., and these must cover all elements of R. It follows that d is a unit of R and the sequence

$$S : 1, 1 + X, 1 + X + X^2, \ldots$$

has period $|R|$.

These conditions are obviously fulfilled in the example: $d = 1$, and $X \equiv 3 \equiv 1$ as well, so 1 and $1 + X = 0$ cover $\mathbb{Z}/2\mathbb{Z}$.

Finally, $0 = (-1, 3)_{3,\text{odd}} = (-1, 5)_{5,\text{odd}}$, and the gcd of these lengths is 2.

One-sidedly linear case

From now on, suppose f and g are monic nonconstant and $f = X - a$ is linear. Then we know that

$$\mathbb{Z}[X]/(f, g) \cong \mathbb{Z}/(\mathrm{Res}(f, g)) = \mathbb{Z}/(g(a)).$$

If $a \equiv 1 \pmod{g(a)}$, then $X = 1$ in the ring R, so of course the sequence S covers R.

Put $s_n = 1 + X + \ldots + X^n$; we have $s_{n+1} = Xs_n + 1$, a linear congruential sequence as used in random number generation.

So, to compute the period of S we can use results about LCSs (e.g. Knuth): we need $X \equiv 1 \pmod{p}$ for all primes p dividing $|R|$, and $X \equiv 1 \pmod{4}$ if 4 divides $|R|$.

These conditions only depend on f and g, so for example if $f = X + 4$ and $g = X + 7$, there are no valid digit sets that give rise to a number system modulo $(X + 4)(X + 7)$.

Conclusion (second try)

Theorem Let $f, g \in \mathbb{Z}[X]$ be monic, nonconstant and coprime with $f = X - a$, $|a| \geq 2$. Let $R = Z[X]/(f, g)$. Then the Chinese Remainder Theorem yields an isomorphism of number systems

$$(\mathbb{Z}[X]/(fg), X, \mathcal{E}) \cong (\mathbb{Z}, a, \mathcal{D}) \times_R (\mathbb{Z}[X]/(g), X, \mathcal{D}')$$

if and only if

- $\mathcal{E}$ is the inverse image of $\mathcal{D} \times \mathcal{D}'$ under the CRT isomorphism;
- $(\mathbb{Z}, a, \mathcal{D})$ and $(\mathbb{Z}[X]/(g), X, \mathcal{D}')$ are number systems with zero cycle lengths L and L', where $(L, L') = |R|$;
- $X \equiv 1 \pmod{p}$ for all primes p dividing $|R|$ and $X \equiv 1 \pmod{4}$ if $4 \mid |R|$;
- there exists $d_0 \in R^*$ such that $d \equiv d_0 \pmod{(f, g)}$ for all $d \in \mathcal{D} \cup \mathcal{D}'$.

Final question

Can anybody give an infinite set of pairwise really coprime polynomials, or even with pairwise resultant ± 1?

My best effort:

$\{X-1,\ X,\ X^2-X+1,\ X^3-X+1,\ X^4-X^3+X^2-X+1,$
$X^5-2X^3+3X^2-2X+1\}.$

And finally:

Gratulálok a születésnapjára!