Note on the analytic representation of integer residues

Summary: We consider a general identity regarding the analytic representation of integer remainders modulo *p*.

Zusammenfassung: Wir betrachten eine allgemeingültige Identität zur analytischen Darstellung ganzzahliger Reste modulo *p*.

By Hieronymus Fischer

1. Introduction

Most commonly, the arithmetic operation 'mod' is used to describe the integer residue r of the division n by 2; in symbols, $r = n \bmod 2$. Therein, the modulo-operation is defined generally by $n \bmod p := n - p\left\lfloor \frac{n}{p} \right\rfloor$, $p \in \mathbb{N}$. Nevertheless, for the special case $p = 2$, sometimes one finds a seemingly more elegant exponential notation according to

(1-1) $$n \bmod 2 = \frac{1-(-1)^n}{2}$$

The question is, whether or not this formula can be extended to integer divisors $p > 2$.

2. Main section

In the following we answer in the affirmative: we show, that there exists a general analytic representation of integer remainders with divisors $p \geq 2$ which goes into formula (1-1) for $p = 2$.

Theorem 2-1

Suppose $n \in \mathbb{Z}$ *and* $p \in \mathbb{N}$*; further let* $\varepsilon_p := e^{\frac{2\pi}{p}i}$ *be the p-th primitive root of unity. Then* $n \bmod p = M_p(n)$*, where the function* $M_p : \mathbb{Z} \to \mathbb{Z}_p$ *is defined by*

(2-1) $$M_p(n) := \frac{1-\varepsilon_p^n}{p} \sum_{\nu=1}^{p-1} \nu \prod_{\mu=1,\, \mu \neq \nu}^{p-1} \left(1 - \varepsilon_p^{n-\mu}\right)$$

<u>Proof:</u>

Since n appears as an exponent of $\varepsilon_p = e^{\frac{2\pi}{p}i}$ only, and so is always a linear argument of the appropriate exponential terms, namely of $\exp\left(\frac{2\pi}{p}i\right)$, it is clear, that $M_p(n)$ is periodically with period p. Hence, it suffices to verify $M_p(n) = n$ for $n = 0, 1, 2, \ldots, p-1$. Since $\varepsilon_p^o = 1$, this holds

true for $n=0$, obviously. Suppose $0<n<p$ now, then the product $\prod_{\mu=1,\,\mu\neq\nu}^{p-1}\left(1-\varepsilon_p^{n-\mu}\right)$ evaluates to zero if and only if $\mu=n$ for one index at least. The latter is evidently true, if $\nu\neq n$. Conversely, the product does not vanish, if and only if $\nu=n$. Given an index n, $0<n<p$, it follows that the very only summand of $\sum_{\nu=1}^{p-1}\nu\prod_{\mu=1,\,\mu\neq\nu}^{p-1}\left(1-\varepsilon_p^{n-\mu}\right)$ which is different from zero is that with index $\nu=n$. Thus, we get $M_p(n)=\frac{n}{p}\left(1-\varepsilon_p^{n}\right)\prod_{\mu=1,\,\mu\neq n}^{p-1}\left(1-\varepsilon_p^{n-\mu}\right)$. As can be easily seen, all terms $\left(1-\varepsilon_p^{\mu}\right)$, $1\le\mu<p$, appears exactly once. Therefore, we can rewrite this formula as $M_p(n)=\frac{n}{p}\prod_{\mu=1}^{p-1}\left(1-\varepsilon_p^{\mu}\right)$.
Since the terms ε_p^{μ}, $0\le\mu<p$ are just the roots of unity of order p, they are also the roots of the cyclotomic polynomial X^p-1, i.e., $X^p-1=\prod_{\mu=0}^{p-1}\left(X-\varepsilon_p^{\mu}\right)=\left(X-1\right)\prod_{\mu=1}^{p-1}\left(X-\varepsilon_p^{\mu}\right)$. It follows $\prod_{\mu=1}^{p-1}\left(X-\varepsilon_p^{\mu}\right)=\frac{X^p-1}{X-1}=1+X+X^2+\ldots+X^{p-1}$, so that $\prod_{\mu=1}^{p-1}\left(1-\varepsilon_p^{\mu}\right)=p$. Subsequently we obtain $M_p(n)=n$ for all n, $0\le n<p$. □

Based on Theorem 2-1 we are now able to represent the digits $a_m a_{m-1}\ldots a_n\ldots a_1 a_0$ of a given non-negative number z in a very explicit manner; only provided, the radix p is a prime number. In fact, according to Theorem 4 1 of References [1] and Theorem 2-1 we obtain the following fairly sophisticated relation

$$a_n=\frac{1-\varepsilon_p^{\binom{z}{p^n}}}{p}\sum_{\nu=1}^{p-1}\nu\prod_{\mu=1,\,\mu\neq\nu}^{p-1}\left(1-\varepsilon_p^{-\mu}\varepsilon_p^{\binom{z}{p^n}}\right)$$

This representation looks nice. Granted, but it also comes across somewhat academically. It is stated here for the sake of completeness only.

If we set $p=2$, then formula (2-1) is identical to the well known formula (1-1). However, for higher p the formulae become more complex. Two examples:

$p=3$, $\varepsilon_3=e^{\frac{2\pi}{3}i}=-\frac{1}{2}+\frac{1}{2}\sqrt{3}\,i$

(2-2) $$n \bmod 3=\frac{1-\varepsilon_3^{n}}{3}\left(\left(1-\varepsilon_3^{n-2}\right)+2\left(1-\varepsilon_3^{n-1}\right)\right)$$

Of course, this can also be written in a non-canonical way; for example:

(2-3) $$n \bmod 3=\frac{1-\varepsilon_3^{n}}{3}\left(3+\left(1-\varepsilon_3^{2}\right)\varepsilon_3^{n}\right)$$

or

(2-4) $$n \bmod 3 = \left(1-\varepsilon_3^n\right)\left(1+\frac{\varepsilon_3^n}{1-\varepsilon_3}\right)$$

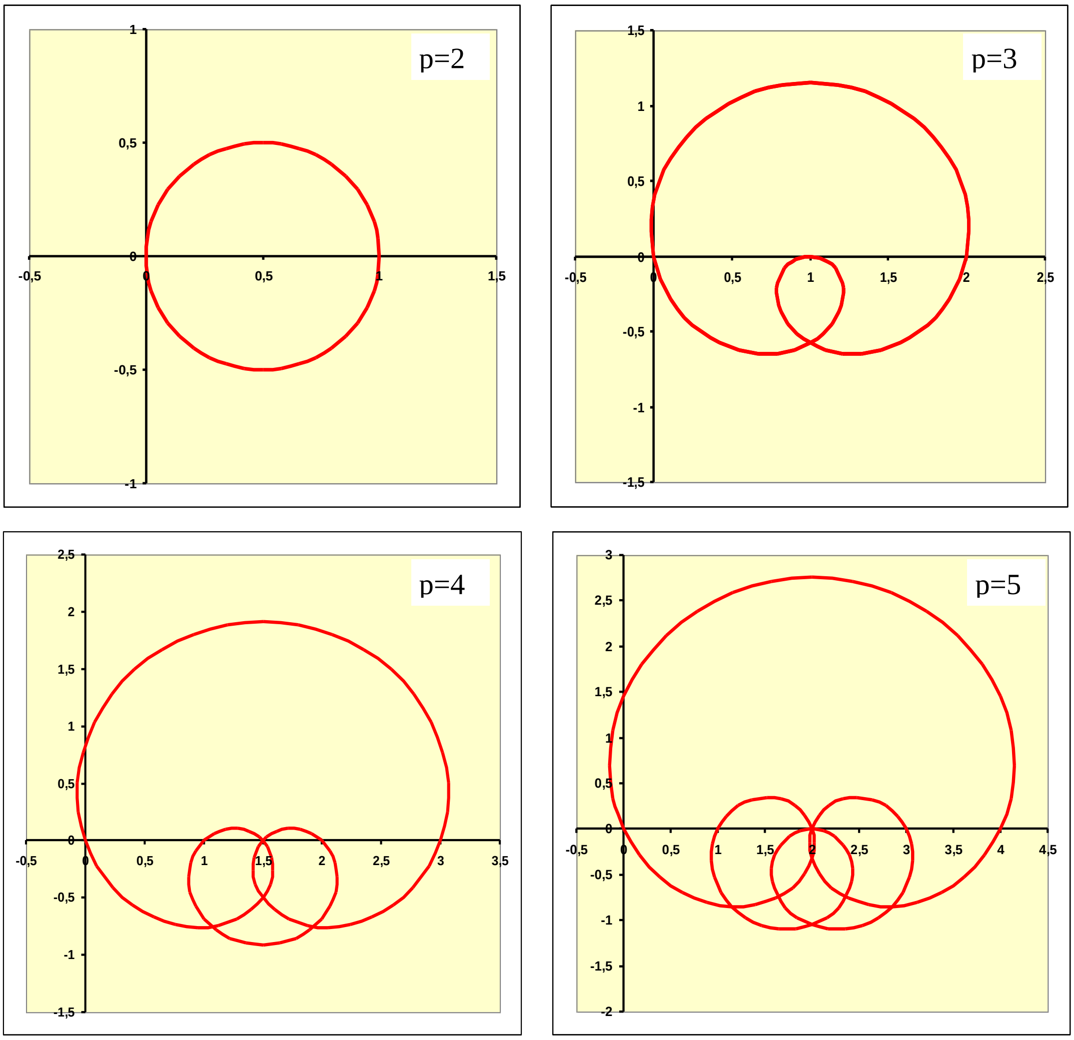
$p=4,\ \varepsilon_4 = e^{\frac{\pi}{2}i} = i$

(2-5) $$n \bmod 4 = \frac{1-\varepsilon_4^n}{4}\cdot \left(\left(1-\varepsilon_4^{n-2}\right)\left(1-\varepsilon_4^{n-3}\right)+2\left(1-\varepsilon_4^{n-1}\right)\left(1-\varepsilon_4^{n-3}\right)+3\left(1-\varepsilon_4^{n-1}\right)\left(1-\varepsilon_4^{n-2}\right)\right)$$

A more compact form of this is given by:

(2-6) $$n \bmod 4 = \frac{1-i^n}{2}\left(\left(1+i\right)(-1)^n+\left(2+i\right)i^n+3\right)$$

If we put a real variable x instead of n and consider the function $M_p(x)$, we get an interesting mapping of the interval $0 \le x < p$ into the complex plane. Since $M_p(x)$ is plainly periodic, the evolving functional mapping results in a closed curve. For p>1 these curves look like $\left(p-1\right)$-fold intertwined circles; putting p=3, for example, we get a curve very similar to a cycloid (s. figures).



Indeed, M_p can be viewed as a mapping of the unity circle. If we set $X := \varepsilon_p^x$ (principal value), formally, and consider $\prod_{\mu=1,\,\mu\neq\nu}^{p-1} \varepsilon_p^{-\mu} = (-1)^{p-1}\,\varepsilon_p^{\nu}$, we obtain

(2-7)
$$\begin{aligned}\tilde{M}_p(X) &:= \frac{1-X}{p}\sum_{\nu=1}^{p-1}\nu\prod_{\mu=1,\,\mu\neq\nu}^{p-1}\varepsilon_p^{-\mu}\left(\varepsilon_p^{\mu}-X\right)\\ &= (-1)^{p-1}\frac{1-X}{p}\sum_{\nu=1}^{p-1}\nu\,\varepsilon_p^{\nu}\prod_{\mu=1,\,\mu\neq\nu}^{p-1}\left(\varepsilon_p^{\mu}-X\right)\end{aligned}$$

With respect to $\sum_{\nu=1}^{p-1}\nu\,\varepsilon_p^{\nu} = \frac{p}{\varepsilon_p - 1}$ we finally get

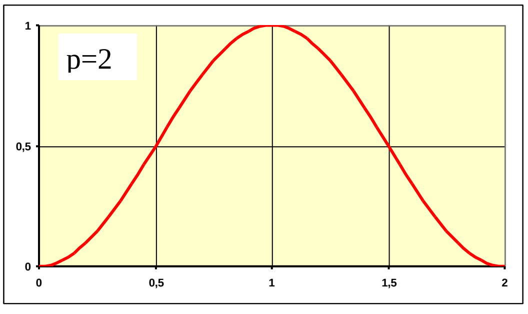
(2-8)
$$\begin{aligned}\tilde{M}_p(X) &= \frac{X-1}{p}\sum_{\nu=1}^{p-1}\nu\,\varepsilon_p^{\nu}\prod_{\mu=1,\,\mu\neq\nu}^{p-1}\left(X-\varepsilon_p^{\mu}\right)\\ &= \frac{X-1}{p}\sum_{\nu=1}^{p-1}\nu\,\varepsilon_p^{\nu}\left(X^{p-2}+O\left(X^{p-3}\right)\right)\\ &= \frac{X^{p-1}}{\varepsilon_p-1}+O\left(X^{p-2}\right)\end{aligned}$$

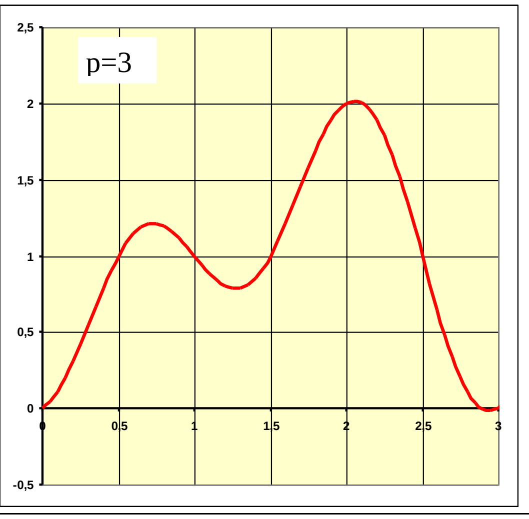
Therewith we have demonstrated that $\tilde{M}_p$ is a polynomial in X of degree $p-1$.

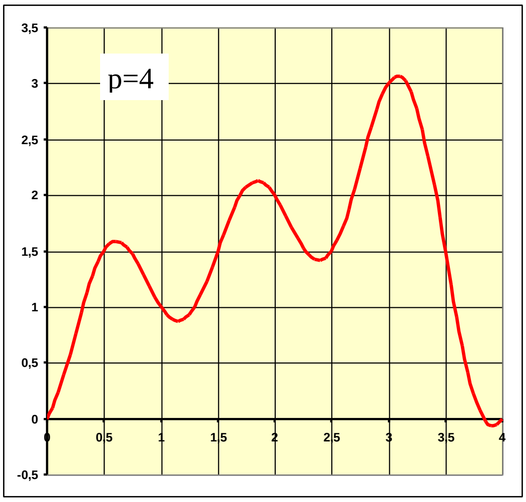
The functional mapping of the real part of $M_p(x)$ has a characteristic shape too. There are always $p-1$ local maxima which is a consequence of the trigonometric structure of $\operatorname{Re}\left(M_p(x)\right)$. With appropriate constants $b_\nu, c_\nu, 1 \le \nu < p$, independent from p, $\operatorname{Re}\left(M_p(x)\right)$ can be written as

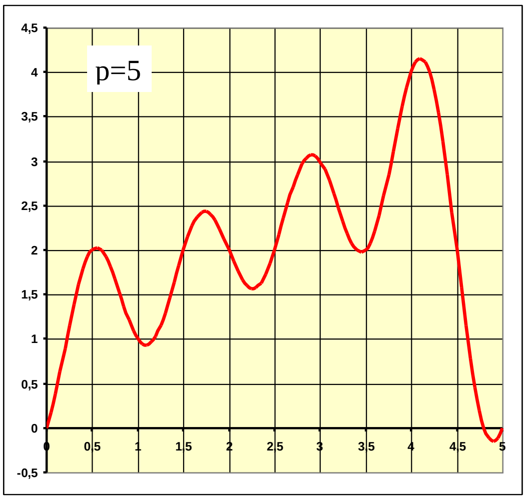
$$b_{p-1}\sin\left(\frac{2\pi}{p}(p-1)x+c_{p-1}\right)+b_{p-2}\sin\left(\frac{2\pi}{p}(p-2)x+c_{p-2}\right)+\ldots+b_1\sin\left(\frac{2\pi}{p}x+c_1\right)$$

The functional mappings of $\operatorname{Re}\left(M_p(x)\right)$ for p=2, 3, 4 and 5 are depicted below.









Besides, the underlying approach presented in Theorem 2-1 can also be generalized into another direction. Suppose, g is a mapping defined for arguments $0 \le n < p$. Then, g can be extended to a function $\tilde{g}$ defined on $\mathbb{Z}$, by simply putting $\tilde{g}(n) := g\left(n \bmod p\right)$. Evidently, $\tilde{g}$ is periodic with period p. Clearly, $\tilde{g}$ can be understood as 'the natural periodic continuation' of g. Now, we define

(2-9) $$M_p^{(g)}(n) := \frac{1}{p} \sum_{\nu=0}^{p-1} g(\nu) \prod_{\mu=0,\ \mu\neq\nu}^{p-1} \left(1-\varepsilon_p^{n-\mu}\right)$$

It can be easily verified, that $M_p^{(g)}(n)$ and $g(M_p(n))$ are identical for $0 \le n < p$, which implies follows $\tilde{g}(n) = M_p^{(g)}(n)$ for all $n \in \mathbb{Z}$ by definition. Thus, it is evident, that $M_p^{(g)}$ also identifies the canonical periodic continuation of g from $\mathbb{Z}_p$ to $\mathbb{Z}$.

References

[1] On the characterization of base-p number representations