An International Journal
computers & mathematics with applications

PERGAMON Computers and Mathematics with Applications 39 (2000) 253–261
www.elsevier.nl/locate/camwa

Powersums Representing Residues $\bmod p^k$, from Fermat to Waring

N. F. BENSCHOP
Amspade Research, NL-5663EZ Geldrop
The Netherlands
benschop@iae.nl

(Received September 1998; accepted December 1998)

Abstract—The ring $Z_k(+,.) \bmod p^k$ with prime power modulus (prime $p > 2$) is analysed. Its cyclic group G_k of units has order $(p-1)p^{k-1}$, and all p^{th} power n^p residues form a subgroup F_k with $|F_k| = |G_k|/p$. The subgroup of order $p-1$, the *core* A_k of G_k, extends Fermat's Small Theorem (FST) to $\bmod p^{k>1}$, consisting of $p-1$ residues with $n^p = n \bmod p^k$. The concept of *carry*, e.g., n' in FST extension $n^{p-1} = n'p + 1 \bmod p^2$, is crucial in expanding residue arithmetic to integers, and to allow analysis of divisors of $0 \bmod p^k$.

For large enough $k \geq K_p$ (critical precision $K_p < p$ depends on p), all nonzero pairsums of core residues are shown to be distinct, up to commutation. The known FLT case$_1$ is related to this, and the set $F_k + F_k \bmod p^k$ of p^{th} power pairsums is shown to cover half of G_k. Yielding main result: each residue $\bmod p^k$ is the sum of at most four p^{th} power residues. Moreover, some results on the generative power $(\bmod p^{k>2})$ of divisors of $p \pm 1$ are derived.

Keywords—Waring, Powersum residues, Primitive roots, Fermat, FLT $\bmod p^k$.

1. INTRODUCTION

The concept of *closure* corresponds to a mathematical operation composing two objects into an object of the same kind. Structure analysis is facilitated by knowing a minimal set of *generators*, to find preserved partitions *viz.* congruences, that allow factoring the closure. For instance, a finite state machine decomposition using preserved (state) partitions, corresponding to congruences of the sequential closure (semigroup) of its state transformations.

A minimal set of *generators* is characterized by *anticlosure*. Then each composition of two generators produces a nongenerator, thus a new element of the closure. These concepts can fruitfully be used for structure analysis of finite residue arithmetic.

For instance positive integer p^{th} powers are closed under multiplication, but no sum $a^p + b^p$ yields a p^{th} power for $p > 2$ (Fermat's Last Theorem, FLT). Apparently p^{th} powers form an efficient set of additive generators. Waring (1770) [1] drew attention to the now familiar representation problem: the sum of how many p^{th} powers suffice to cover all positive integers. Lagrange (1772) [1] and Euler showed that four squares suffice. The general problem is as yet unsolved.

0898-1221/00/$ - see front matter Typeset by $\mathcal{A}_{\mathcal{M}}\mathcal{S}$-TeX
PII: S0898-1221(00)00080-8

Our aim is to show that four p^{th} power residues $\bmod p^k$ (prime $p > 2$, $k > 0$ large enough) suffice to cover all p^k residues under addition. As shown in [2,3], the analysis of residues $a^p + b^p \bmod p^k$ is useful here, because under modulus p^k the p^{th} power residues coprime to p form a proper multiplicative subgroup $F_k \doteq \{n^p\} \bmod p^k$ of the group of units $G_k(.) \bmod p^k$, with $|F_k| = |G_k|/p$. The value range $F_k + F_k \bmod p^k$ is studied.

Units group G_k, consisting of all residues coprime to p, is in fact known to be cyclic for all $k > 0$ [4]. There are p^{k-1} multiples of $p \bmod p^k$, so its order $p^k - p^{k-1} = (p-1)p^{k-1}$ is a product of two coprime factors, hence we have

$$G_k = A_k B_k \text{ is a direct product of subgroups, with } |A_k| = p - 1 \text{ and } |B_k| = p^{k-1}. \tag{1}$$

The *extension* subgroup B_k consists of all p^{k-1} residues $1 \bmod p$. And in *core* subgroup A_k, of order $|A_k| = p - 1$ independent of k, each n satisfies $n^p = n \bmod p^k$, denoted as $n^p \equiv n$. Hence, core A_k is the extension of Fermat's Small Theorem (FST) $\bmod p$ to $\bmod p^k$ for $k > 1$. For more details, see [3].

By a coset argument, the nonzero corepairsums in $A_k + A_k$, for large enough k, are shown to be all distinct in G_k, apart from commutation (Theorem 2.1). This leads to set $F_k + F_k$ of p^{th} power pairsums covering almost half of G_k, the maximum possible in a commutative closure, and clearly related to Fermat's Last Theorem (FLT) about the anticlosure of the sum of two p^{th} powers.

Additive analysis of the roots of $0 \bmod p^2$, as sums of three p^{th} power residues, via the generative power of divisors of $p \pm 1$ (Theorem 3.1), yields our main result (Theorem 3.2): the sum of at most four p^{th} power residues $\bmod p^k$ covers all residues, a *Waring-for-residues* result. Finite semigroup and ring analysis beyond groups and fields is essential, due the crucial role of divisors of zero.

2. CORE INCREMENTS AS COSET GENERATORS

The two component groups of $G_k \equiv A_k.B_k$ are residues $\bmod p^k$ of two monomials: the *core* function $A_k(n) = n^{q_k}$ ($q_k = |B_k| = p^{k-1}$) and *extension* function $B_k(n) = n^{|A_k|} = n^{p-1}$. Core function $A(n)$ has odd degree with a q-fold zero at n=0, and is monotone increasing for all n. Its first difference $d_k(n) = A_k(n+1) - A_k(n)$ of even degree has a global minimum integer value of 1 at $n = 0$ and $n = -1$, and symmetry centered at $n = -1/2$. Thus, integer equality $d_k(m) = d_k(n)$ for $m \neq n$ holds only if $m + n = -1$, called one-complements.

Hence, the next definition of a *critical precision* $k = K_p$ for residues with the same symmetric property is relevant for every odd p, not necessarily prime. Core difference $d_k(n)$ is $1 \bmod p$, so it is referred to as *core increment* $d_k(n)$. To simplify notation, the precision index k is sometimes omitted, with $\equiv$ denoting equivalence $\bmod p^k$, especially since core A_k has order $p-1$ independent of k.

Define critical precision K_p as the smallest k for which the *only* equivalences among the core-increments $d_k(n) \bmod p^k$ are the above described one-complement symmetry for $n \bmod p$, so these increments are all distinct for $n = 1 \ldots (p-1)/2$.

Notice that K_p depends on p, for instance K_p=2 for $p \leq 7$, $K_{11} = 3$, $K_{13} = 2$, and the next $K_p = 4$ for $p = 73$. Upperbound $K_p < p$ will be derived in the next section (Lemma 3.1c), so no 'Hensel lift' [5] occurs. Notice that $|F_k|/|A_k| = p^{k-2}$, so that $A_2 = F_2 = \{n^p\} \bmod p^2$.

LEMMA 2.1. *Integer core-function* $A_k(n) = n^{p^{k-1}}$ *and its increment* $d_k(n) = A_k(n+1) - A_k(n)$ *both have period* p *for residues* $\bmod p^k$ *with:*

(a) *odd symmetry* $A_k(m) \equiv -A_k(n)$ *at complements* $m + n = 0 \bmod p$,
(b) *even symmetry* $d_k(m) \equiv d_k(n)$ *at one-complements* $m + n = -1 \bmod p$,
(c) *let* D_2 *be the set of distinct increments* $d_2(n) \bmod p^2$ *of* $F_2 = A_2$ *for* $0 < n \leq (p-1)/2$, *then there are* $|F_k + F_k \backslash 0\ | = |F_k|\,|D_2| = |G_k|\,|D_2|/p$ *nonzero* p^{th} *power pairsums* $\bmod p^k$ *(any* $k > 1$*).*

PROOF.

(a) Core function $A_k(n) = n^{q_k} \bmod p^k$ ($q_k = p^{k-1}$, $n \neq 0, -1 \bmod p$) has $p-1$ distinct residues for each $k > 0$, satisfying $(n^q)^p = n^q \bmod p^k$, with $A_k(n) = n \bmod p$ due to FST. Apparently, including $A_k(0) = 0$, we have: $A_k(n+p) = A_k(n) \bmod p^k$ for each $k > 1$, with *period* p in n. And $A_k(n)$ of odd degree $q = q_k$ has *odd symmetry* because

$$A_k(-n) = (-n)^q = -n^q = -A_k(n) \bmod p^k.$$

(b) Increment $d_k(n) = A_k(n+1) - A_k(n) \bmod p^k$ also has period p because

$$d_k(n+p) = (n+p+1)^{q_k} - (n+p)^{q_k} = (n+1)^{q_k} - n^{q_k} = d_k(n) \bmod p^k.$$

This yields residues 1 mod p in extension group B_k. It is an even degree polynomial, with leading term $q_k.n^{q_k-1}$, and *even symmetry*

$$d_k(n-1) = n^{q_k} - (n-1)^{q_k} = -(-n)^{q_k} + (-n+1)^{q_k} = d_k(-n),$$

so $d_k(m) = d_k(n) \bmod p^k$ for one-complements: $m + n = -1 \bmod p$.

(c) Write F for F_k (*any* $k > 1$), the subgroup of p^{th} power residues mod p^k in units group G_k. Then subgroup closure $FF = F$ implies $F{+}F = F(F{+}F) = F(F{-}F)$, since $F{+}F = F{-}F$ due to -1 in F for odd prime $p > 2$. So nonzero pairsum set $F+F \setminus 0$ is the disjoint union of cosets of F in G, as generated by differences $F - F$. Due to (1): $G_k = A_kB_k = F_kB_k$, where $A_k \subseteq F_k$, it suffices to consider only differences 1 mod p, hence in extension group $B = B_k$, that is, in $(F - F) \cap B$.

This amounts to $|D_2| \leq h = (p-1)/2$ distinct increments $d_2(n)$, for $n = 1 \ldots h$ due to even symmetry (b), and excluding $n = 0$ involving noncore $A_2(0) = 0$. These $|D_2|$ cosets of F_k in G_k yield: $|F_k + F_k \setminus 0\,| = |F_k|\,|D_2|$, where $|F_k| = |G_k|/p = (p-1)p^{k-2}$ and $|D_2| \leq (p-1)/2$. ∎

For many primes $K_p = 2$, so $|D_2| = (p-1)/2$, and Fermat's p^{th} power residue pairsums cover almost half the units group G_k, for any precision $k > 1$. But even if $K_p > 2$, with $|D_2| < (p-1)/2$, this suffices to express each residue mod p^k as the sum of at most four p^{th} power residues (Theorem 3.2), as shown in the next section.

THEOREM 2.1. *For a, b in core A mod p^k, and $k \geq K_p$*

all nonzero pairsums $a + b \bmod p^k$ are distinct, apart from commutation, so

$$|(A+A)\backslash 0| = \frac{1}{2}|A|^2 = \frac{(p-1)^2}{2}.$$

PROOF. Core $A_k \bmod p^k$ (*any* $k > 1$), here denoted by A as subgroup of units group G, satisfies $AA = A$ so the set of all core pairsums can be factored as $A{+}A = A(A{+}A)$. Hence, the nonzero pairsums are a (disjoint) union of the cosets of A generated by $A + A$. Since $G = AB$ with $B = \{n = 1 \bmod p\}$, there are $|B| = p^{k-1}$ cosets of A in G. Then intersection $D = (A+A) \cap B$ of all residues 1 mod p in $A + A$ generates $|D|$ distinct cosets of A in G.

Due to -1 in core A, we have $A = -A$ so that $A + A = A - A$. View set A as function values $A(n) = n^{|B|} \bmod p^k$, with $A(n) = n \bmod p$ $(0 < n < p)$. Then successive core increments $d(n) = A(n+1) - A(n)$ form precisely intersection D, yielding all residues 1 mod p in $A + A = A - A$. Distinct residues $d(n)$ generate distinct cosets, so by definition of K_p there are for $k \geq K_p:\ |D| = (p-1)/2$ cosets of core A generated by $d(n) \bmod p^k$.

3. CORE EXTENSIONS FROM A_k TO F_k, AND THEIR PAIRSUMS $\bmod p^k$

Extension group $B \bmod p^k$, with $|B| = p^{k-1}$ has only subgroups of order p^e $(e = 0 \ldots k-1)$. So $G \equiv AB$ (1) has k subgroups $X^{(e)}$ that contain core A, called *core extensions*, of order $|X^{(e)}| = (p-1)p^e$, with core $A = X^{(0)}$, $F = X^{(k-2)}$, and $G = X^{(k-1)}$.

Now $p+1$ generates B of order p^{k-1} in G_k [3, Lemma 2], and similarly

$$p^i + 1 \text{ of period } p^{k-i} (i = 1 \ldots k-1) \text{ in } G \text{ generate the } k-1 \text{ subgroups of } B. \tag{2}$$

Let $Y^{(e)} \subseteq B$, of order p^e, then all core extensions are cyclic with product structure

$$X^{(e)} \equiv AY^{(e)} \text{ in } G(.), \text{ where } |A| \text{ and } |Y^{(e)}| \text{ are relative prime.}$$

Using (2) with $k - i = e$ yields

$$Y^{(e)} \equiv \left(p^{k-e}+1\right)^* \equiv \left\{mp^{k-e}+1\right\} \bmod p^k \,(\text{all } m). \tag{2'}$$

As before, using residues $\bmod p^k$ for any $k > 1$: $D = (A - A) \cap B$ contains the set of core increments. Then Theorem 2.1 on core pairsums $A + A$ is generalized as follows (Lemma 3.1a) to the set $X + X$ of core extension pairsums $\bmod p^j$ $(j > 1)$, with $F + F$ (*Fermat sums*) for $j = k - 2$.

Extend Fermat's Small Theorem FST: $n^{p-1} = 1 \bmod p$ to $n^{p-1} = n'p + 1 \bmod p^2$, which defines the FST-*carry* n' of $n < p$. This yields an efficient *core generation* method (b) to compute $n^{p^i} \bmod p^{i+1}$, as well as a proof (c) of critical precision upperbound $K_p < p$.

LEMMA 3.1. *For core increments $D_k = (A_k - A_k) \cap B_k$ in $G_k = A_k B_k \bmod p^{k>1}$ (prime $p > 2$), p^{th} power residues set $F_k = \{n^p\} \bmod p^k$, and X_k any core extension $A_k \subseteq X_k \subseteq F_k$,*

(a) *$X_k + X_k \equiv X_k D_k$, so core-increments D_k generate the X_k-cosets in $X_k + X_k$,*
(b) *$[n^{p-1}]^{p^{i-1}} = n'p^i + 1 \bmod p^{i+1}$, where FST-carry n' of n does not depend on i, and $n^{p^i} = [n'p^i + 1] n^{p^{i-1}} \bmod p^{i+1}$,*
(c) *for $k = p$: $|D_p| = (p-1)/2 \bmod p^p$, so critical precision $K_p < p$.*

PROOF a. Write X for $X_k^{(e)}$, then as in Theorem 2.1: $X + X = X - X = (X - X)X$. For residues $\bmod p^k$, we seek intersection $(X - X) \cap B$ of all distinct residues $1 \bmod p$ in B that generate the cosets of X in $X + X \bmod p^k$. By (2,2′) core extension $X = AY = A\{mp^{k-e} + 1\}$. Discard terms divisible by p (are not in B), then $(X + X) \cap B = (A + A) \cap B = (A - A) \cap B = D$ for each core extension. So $A + A$ and $X + X$ have the same coset generators in G_k, namely the core increment set $D = D_k \subset B_k$.

PROOF b. Notice successive cores satisfy by definition $A_{i+1} = A_i \bmod p^i$. In other words, each p^{th} power step $i \to i+1$: $[n^{p^i}]^p$ produces one more significant digit (msd) while fixing the i less significant digits (lsd). Now $n^{p-1} = n'p + 1 \bmod p^2$ has p^{th} power residue $[n^{p-1}]^p = n'p^2 + 1 \bmod p^3$, implying lemma part (b) by induction on i in $[n^{p-1}]^{p^i}$.

This yields an efficient *core generation* method. Denote $f_i(n) = n^{p^i}$, with $n < p$, then

$$f_i(n) = n^{p^i} = [n^p]^{\,p^{i-1}} = \left[nn^{p-1}\right]^{\,p^{i-1}} = f_{i-1}(n)\left[n'p^i + 1\right] \bmod p^{i+1}, \text{ implying} \tag{3}$$
$$f_i(n) = f_{i-1}(n) \bmod p^i, \text{ next core msd } f_{i-1}(n)n'p^i = nn'p^i \neq 0 \bmod p^{i+1}. \tag{3'}$$

Notice that by FST: $f_k(n) = n \bmod p$, for all $k \geq 0$, and $0 < n < p$ implies $n' \neq 0 \bmod p$.

PROOF c. In (a), take $X_k = F_p$ and notice that $F_p + F_p = F_p - F_p \bmod p^p$ contains h distinct integer increments

$$e_1(n) = (n+1)^p - n^p < p^p, \tag{4}$$

which are 1 mod p^p, hence in B_p: they generate h distinct cosets of core A_p in $G_p = A_pB_p \bmod p^p$, although they are not core A_p increments. Repeated p^{th} powers n^{p^i} in constant p-digit precision yield increments $e_i(n) = (n+1)^{p^i} - n^{p^i} \bmod p^p$, which for $i = p-1$ produce the increments of core $A_p \bmod p^p$.

Distinct increments $e_i(n) \neq e_i(m) \bmod p^p$ remain distinct for $i \to i+1$, shown as follows.

For nonsymmetric $n,\ m < p$ (Lemma 2.1b) let increments e_i satisfy

$$e_i(n) = e_i(m) \bmod p^j \text{ for some } j < p \tag{5}$$

and

$$e_i(n) \neq e_i(m) \bmod p^{j+1}. \tag{5$'$}$$

Then for $i \to i+1$ the same holds, since $e_{i+1}(x) = [f_i(x+1)]^p - [f_i(x)]^p$ where x equals n and m, respectively. Because in $(5, 5')$ each of the four $f_i()$ terms has form $bp^j + a \bmod p^{j+1}$ where the, respectively, $a < p^j$ yield (5), and the, respectively, msd's $b < p$ cause inequivalence $(5')$. Then

$$f_{i+1}() = \left(bp^j + a\right)^p = a^{p-1}bp^{j+1} + a^p \bmod p^{j+2} = a^p \bmod p^{j+1}, \tag{6}$$

which depends only on a, and not on msd bp^j of $f_i()$. This preserves equivalence (5) mod p^j for $i \to i+1$, and similarly inequivalence $(5')$ mod p^{j+1} because, depending only on the respective $a \bmod p^j$, equivalence at $i+1$ would contradict $(5')$ at i. Cases $i < j$ and $i \geq j$ behave as follows.

For $i < j$, the successive differences

$$e_i(n) - e_i(m) = y_i p^j \neq 0 \bmod p^{j+1} \dots \tag{6$'$}$$

vary with i from 1 to $j-1$, and by $(3')$ the core residues $f_i() \bmod p^i$ settle for increasing precision i.

So initial inequivalences mod p^p (4), and more specifically mod p^{j+1} (5), are preserved.

And for all $i \geq j$, the differences $(6')$ are some constant $cp^j \neq 0 \bmod p^{j+1}$, again by $(3')$. Hence by induction, base (4) and steps (5,6): core $A_p \bmod p^p$ has $h = (p-1)/2$ distinct increments, so critical precision $K_p < p$. ∎

Apparently, K_p is determined already by the initial integer increments $e_1(n) < p^p$ $(0 < n < p)$, as the minimum precision k for which nonsymmetric $n, m < p$ (so $n + m \neq p-1$) have $e_1(n) \neq e_1(m) \bmod p^k$.

For instance, p=11 has $K_p = 3$, and mod p^3 we have $h = 5$ distinct core increments, in base 11 code: $d_3(1\dots9) = \{4a1,\ 711,\ 871,\ 661,\ 061,\ 661,\ 871,\ 711,\ 4a1\}$ so core A_3 has the maximal five cosets generated by increments $d_3(n)$. Equivalence $d_2(4) = d_2(5) = 61 \bmod p^2$ implies 661 and 061 to be in the same F-coset in G_3. In fact, 061.601=661 (base 11) with 601 in $F \bmod p^3$, as are all p residues of form $\{mp^2+1\} = (p^2+1)^* \bmod p^3$.

As example of Lemma 3.1c, with $p = 11$ and up to three-digit precision

$$\{n^p\} = \{001,\ 5a2,\ 103,\ 274,\ 325,\ 886,\ 937,\ aa8,\ 609,\ 0aa\},$$
$$\text{core } A_3 = \{001, 4a2,\ 103,\ 974,\ 525,\ 586,\ 137,\ 9a8,\ 609,\ aaa\},$$

$e_1(4) = 325 - 274 = 061$ and

$e_1(5) = 886 - 325 = 561$ with FST-carries: $4^{p-1} = a1,\ 5^{p-1} = 71,\ 6^{p-1} = 51$ so:

$e_2(4) = 525 - 974 = 661$ by rule (3) yields: $5^{p^2} - 4^{p^2} = [701]5^p - [a01]4^p = 661,$

$e_2(5) = 586 - 525 = 061$ derived by (3) as: $6^{p^2} - 5^{p^2} = [501]6^p - [701]5^p = 061.$

Notice second difference $e_2(5) - e_2(4) = 061 - 661 = 500$ equals $e_1(5) - e_1(4) = 561 - 061 = 500$ by Lemma 3.1c.

With $|F| = |G|/p$ and $|D_k|$ equal to $(p-1)/2$ for large enough $k < p$, the nonzero p^{th} power pairsums cover nearly half of G. It will be shown that four p^{th} power residues suffice to cover not only $G \bmod p^k$, but all residues $Z \bmod p^k$. In this additive analysis, we use the following.

NOTATION. S_{+t} is the set of all sums of t elements in set S, and $S + b$ stands for all sums $s + b$ with $s \in S$.

Extension subgroup B is much less effective as additive generator than F. Notice that $B \equiv \{np+1\}$ so that $B + B \equiv \{mp+2\}$, and in general $B_{+i} \equiv \{np+i\}$ in G, denoted by N_i, the subset of G which is $i \bmod p$. They are also the (additive) *translations* $N_i \equiv B - 1 + i$ $(i < p)$ of B. Then $N_1 \equiv B$, while only $N_0 \equiv \{np\}$ is not in G, and $N_i + N_j \equiv N_{i+j}$, corresponding to addition $\bmod p$.

Coresums A_{+i} in general satisfy the next inclusions, implied by $0 \in A_{+2} \equiv A + A$,

$$\text{for all } i \geq 1 : A_{+i} \subseteq A_{+(2+i)} \quad \text{and} \quad F_{+i} \subseteq F_{+(2+i)}.$$

F_{+3} covering all nonzero multiples $mp \bmod p^k$ $(k \geq 2)$ in N_0 is related to a special result on the number 2 as generator. For instance, a computer scan showed $2^p \neq 2 \bmod p^2$ $(2 \notin A_2)$ for all primes $p < 10^9$ except 1093 and 3511, although inequality does hold $\bmod p^3$ for all primes (shown next). Notice that only 2 divides $p-1$ for each odd prime p, so the two-cycle $C_2 = \pm 1$ is the only cycle common to all cores for $p > 2$. The generative power of 2 might be related to it being a divisor of $p-1$ and $p+1$, for all $p > 2$.

Regarding the known unsolved problem of a simple rule to find primitive roots of $1 \bmod p^k$, consider the divisors r of $p^2 - 1 = (p-1)(p+1)$ as *generators*.

Recall that by (1) units group $G_k = A_k B_k \bmod p^k$ has core subgroup A_k of order $p-1$, for any precision $k > 0$, and extension group $B_k = (p+1)^*$ of all p^{k-1} residues $1 \bmod p$, generated by $p+1$ [3, Lemma 2]. In fact, $p-1$ generates all $2p^{k-1}$ residues $\pm 1 \bmod p^k$, including B_k.

In multiplicative cyclic group G_k of order $(p-1)p^{k-1}$, it stands to reason to look for generators of G_k (primitive roots of $1 \bmod p^k$) among the divisors of such powerful generators as $p \pm 1$, or similarly of $p^2 - 1 = (p-1)(p+1)$. Given prime structure $p^2 - 1 = \prod_i p_i^{e_i}$, there are $\prod_i (e_i + 1)$ divisors, forming a lattice, which is not Boolean since factor 2^2 makes $p^2 - 1$ nonsquarefree.

Notice that for each unit n in G_k, we have n^{p-1} in B_k, and $n^{p^{k-1}}$ in core A_k, while intersection $A_k \cap B_k = 1 \bmod p^k$, the single unity of G_k. No generator g of G_k can be in core A_k, since $|g^*| = (p-1)p^{k-1}$, while the order $|n^*|$ of $n \in A_k$ divides $|A_k| = p-1$. Hence, p must divide the order of any noncore residue. If $n < p^k$, then n can be interpreted both as integer and as residue $\bmod p^k$. It turns out that analysis modulo p^3 suffices to show that the divisors r of $p \pm 1$ are outside core, so $r^p \neq r \bmod p^3$: a necessary but not sufficient condition for a primitive root. This amounts to quadratic analysis of an extension of Fermat's Small Theorem (FST) on p^{th} power residues, including two carry digits (base p).

THEOREM 3.1. DIVISORS OF $p \pm 1$.

$$\textit{If } r > 1 \textit{ divides } p^2 - 1, \textit{then } r^p \neq r \bmod p^k (k \geq 3).$$

PROOF. $r^p \neq r \bmod p^k$ implies inequality $\bmod p^{k+1}$. With $A_2 = F_2 = \{n^p\} \bmod p^2$, so each p^{th} power is in core $A_2 \bmod p^2$, it suffices to show $r^p \neq r \bmod p^3$. Factorize $p^2 - 1 = rs$, with positive integer cofactors r and s. Then $rs = -1 \bmod p^2$, so opposite signed cofactors $\{r, -s\}$ or $\{-r, s\}$ form an inverse pair $\bmod p^2$. Inverses in a finite group G have equal order (*period*) in G, with order two automorphism $n \leftrightarrow n^{-1}$. So orders $|r^*|$ and $|(-s)^*|$ are equal in G_2.

Notice $rs = p^2 - 1$ is not in core A_3, where $-1 \bmod p^3$ is the only core residue that is $-1 \bmod p$, since the $p-1$ core residues $n^{|B_k|}$ of A_k are distinct $\neq 0 \bmod p$ (FST). In fact, $(rs)^p = (p^2-1)^p = -1 \bmod p^3$ and no smaller exponent yields this. So $p^2 - 1 = rs$ has order $2p$ in G_3, generating all $2p$ residues $\pm 1 \bmod p^2$, with inverse pair $\{r^p, -s^p\}$ of equal order in G_3. Core A_3 is closed under multiplication, so at most one cofactor of noncore product rs can be in core. In fact, neither is in core A_3, so both r^{p-1} and s^{p-1} are $\neq 1 \bmod p^3$, seen as follows.

By $G_3 = A_3B_3$ (1): each $n \in G_3$ has product form $n = n'n'' \bmod p^3$ of two components, with n' in core A_3 and n'' in extension group B_3. Then $r^p(-s)^p = 1 \bmod p^3$, where r^p and $-s^p$ as inverse pair in G_3 have equal order, and each component forms an inverse pair of equal orders in A_3 and B_3 (coprime), respectively. The latter must divide $|B_3| = p^2$, and discarding order 1 (both r, s cannot be in core, as shown) their common order is p or p^2. For any unit n the order of n^p divides that of n, so p dividing the common order of r^p and s^p implies p dividing also those of r and s, hence cofactors r and s of $p^2 - 1$ are both outside core A_3. ∎

NOTES.

1. A generator $g < p$ of G_2, so $|g^*| = (p-1)p$, also generates $G_k \bmod p^{k>2}$ of order $(p-1)p^{k-1}$ [4].
2. Cofactors r, s in $rs = p^2 - 1 = (p-1)(p+1)$ have equal period in G_3, up to a factor of 2, so only $r \leq p+1$ need be inspected for periodic analysis. Recall exceptions $p = 1093, 3511$ with $2^p = 2 \bmod p^2$, the only two primes $p < 10^9$ with this property. Of the 79 primes up to 401, there are seven primes with $r^p = r \bmod p^2$ for some divisor $r \mid p^2 - 1$ and cofactor s, namely

$$p(r):\ 11(3),\ 29(14),\ 37(18),\ 181(78),\ 257(48),\ 281(20),\ 313(104).$$

3. A generator g of G_k is outside core, but $g \mid p \pm 1$ (Theorem 3.1) does not guarantee $G_k = g^*$.
4. However, computational evidence seems to suggest the next conjecture.

   CONJECTURE. *At least one divisor $g \mid p \pm 1$ (prime $p > 2$) generates G_k, or half of G_k with -1 missing: then complements $-n \bmod p^k$ yield the other half of G_k (e.g., $p = 73:\ G_3 = \pm 6^* = \pm 12^*$).*
5. The theorem also holds for divisors of $p^2 + 1$, obviating "up to a factor 2" in the proof.

For odd prime p holds: 2 divides both $p - 1$ and $p+1$, and 3 divides one of them, hence the following.

COROLLARY 3.1. *For prime p (including $p = 2$), $k \geq 3$ and $n = 2, 3$*

$$n^p \neq n \bmod p^k, \text{ and in fact } \pm \{n,\ n^{-1}\} \bmod p^k \text{ are outside core } A_{k>2} \text{ for every odd prime.}$$

In set notation: quadruple $Q(r) = \pm \{r,\ r^{-1}\},\ r \mid (p \pm 1)$, and $k \geq 3$ imply $Q(r) \cap A_k = \emptyset$.
Moreover, the product of $r \notin A_k$ with a core element is outside core: $[\ Q(r)A_k\ ] \cap A_k = \emptyset$.

Hence, 2 is not in core $A \bmod p^k$ for any prime $p > 2$. This relates to $p - 1$ having divisor 2 for all p, and $C_2 = \{-1, 1\}$ as the only common subgroup of $Z(.) \bmod p^k$ for all primes $p > 2$. And 2 not in core implies the same for its complement and inverse, -2 and $\pm\ 2^{-1}$.

Notice that $N_0 \bmod p^k$ consists of all multiples mp of p, and their base p code ends on '0', so $|N_0| = p^{k-1}$. In fact, N_0 consists of all divisors of 0, the maximal nilpotent subsemigroup of $Z(.) \bmod p^k$, the semigroup of residue multiplication. For prime p, there are just two idempotents in $Z(.) \bmod p^k$: 1 in G and 0 in N_0, so G and N_0 are complementary in Z, noted $N_0 \equiv Z \setminus G$.

For prime $p > 2$, consider integer p^{th} power function $F(n) = \{n^p\}$, with F_k denoting set $F(n) \bmod p^k$ for all $n \neq 0 \bmod p$, and core function $A_k(n) = n^{p^{k-1}}$, with core $A_2 = F_2$. Multiples mp ($m \neq 0 \bmod p$) are not p^{th} power residues (which are 0 $\bmod p^2$), thus are not in F_k for any $k > 1$. But they are sums of three p^{th} power residues: $mp \in F_{+3} \bmod p^k$ for any $k > 1$, shown next. In fact, due to FST we have $F(n) = n \bmod p$ for all n, so $F(r)+F(s)+F(t) = r+s+t \bmod p$, which for a sum 0 $\bmod p$ of positive triple r, s, t implies $r + s + t = p$.

LEMMA 3.2. *For* $m \neq 0 \bmod p$: $mp \in F_{+3} \bmod p^{k>1}$, *hence*

each multiple $mp \bmod p^{k>1}$ *outside* F_k *is the sum of three* p^{th} *power residues (in* F_k*).*

PROOF. Analysis $\bmod p^2$ suffices, because each $mp \bmod p^{k>1}$ is reached upon multiplication by F_k, due to (.) distributing over (+). Core A_k has order $p-1$ for any $k>0$, and $F_2 = A_2$ implies powersums $F_2 + F_2 + F_2 \bmod p^2$ to be sums of three core residues.

Assume $A(r) + A(s) + A(t) = mp \neq 0 \bmod p^2$ for some positive r, s, t with $r + s + t = p$.

Such $mp \notin A_2$ generates all $|A_2 mp| = |A_2| = p - 1$ residues in $N_0 \setminus 0 \bmod p^2$. And for each prime $p > 2$, there are many such coresums mp with $m \neq 0 \bmod p$, seen as follows.

Any positive triple (r, s, t) with $r + s + t = p$ yields, by FST, coresum $A(r) + A(s) + A(t) = r + s + t = p \bmod p$, hence with a coresum $mp \bmod p^2$. If $m = 0$, then this solves FLT case$_1$ for residues $\bmod p^2$, for instance the cubic roots of $1 \bmod p^2$ for each prime $p = 1 \bmod 6$, see [3].

Nonzero m is the dominant case for any prime $p > 2$. In fact, normation upon division by one of the three core terms in units group G_2 yields one unity core term, say $A(t) = 1 \bmod p^2$, hence $t = 1$. Then $r + s = p - 1$ yields $A(r) + A(s) = mp - 1 \bmod p^2$, where $0 < m < p$.

There are $1 \leq |D_2| \leq (p-1)/2$ distinct cosets of $F_2 = A_2$ in G_2 (Lemmas 2.1 and 3.1), yielding as many distinct core pairsums $mp - 1 \bmod p^2$ in set $A_2 + A_2$.

For most primes, take $r = s$ equal to $h = (p-1)/2$ and $t = 1$, with core residue $A(h) = h = -2^{-1} \bmod p$. Then $2A(h) + 1 = mp = 0 \bmod p$, with summation indices $h + h + 1 = p$. For instance, $p = 7$ has $A(3) = 43 \bmod 7^2$ (base 7), and $2A(3) + 1 = 16 + 1 = 20$.

If for some prime p, we have in this case $m = 0 \bmod p$, then $2A(h) = -1 \bmod p^2$, hence $A(h) = h^p = h \bmod p^2$, and thus, also $A(2) = 2^p = 2 \bmod p^2$. In such rare cases (for primes $< 10^9$ only $p = 1093$ and $p = 3511$), a choice of other triples $r + s + t = p$ exists for which $A(r) + A(s) + A(t) = mp \neq 0 \bmod p^2$, as just shown.

For instance, $2^p = 2 \bmod p^2$ for p=1093, but $3^p = 936p + 3 \bmod p^2$ so that instead of $(h, h, 1)$, one applies $(r, s, 1)$ where $r = (p-1)/3$ and $s = (p-1)2/3$. And $p = 3511$ has $3^p = 21p+3 \bmod p^2$, while $3|p-1$ allows a similar index triple with coresum $mp \neq 0 \bmod p^2$.

Lemma 3.2 leads to the main additive result for residues in ring $Z[+,.] \bmod p^k$

each residue $\bmod p^k$ is the sum of at most four p^{th} power residues.

In fact, with subgroup $F = \{n^p\}$ of G in semigroup $Z(.) \bmod p^k$, subsemigroup $N_0 \equiv \{mp\}$ of divisors of zero, and extension group $B \equiv N_1 \equiv N_0{+}1$ in G, we have the following.

THEOREM 3.2. *For residues* $\bmod p^k$ *(*$k \geq 2$*, prime* $p > 2$*)*

$$Z \equiv N_0 \cup G \equiv F_{+3} \cup F_{+4}.$$

PROOF. Analysis $\bmod p^2$ suffices, by extension Lemma 3.1, and by Lemma 3.2 all nonzero multiples of p are $N_0 \setminus 0 \equiv F_{+3}$, while $0 \in F_{+2}$ because $-1 \in F$. Hence, $F_{+2} \cup F_{+3}$ covers N_0. Adding an extra term F yields $F_{+3} \cup F_{+4} \supseteq N_0 + F$, which also covers $AN_0 + A \supseteq A(N_0 + 1) = AB = G$ because $1 \in A$ and $A \subseteq F$, so all of $Z \equiv N_0 \cup G$ is covered. ∎

NOTES.

1. Case $p = 3$ is easily verified by complete inspection as follows. Analysis $\bmod p^3$ (Theorem 3.2) is rarely needed; for instance, condition $2^p \neq 2 \bmod p^2$ holds for all primes $p < 10^9$ except for the two primes 1093 and 3511. So $\bmod p^2$ will suffice for $p = 3$; moreover, $F = A \bmod p^2$.

   Now $F \equiv \{-1, 1\} \equiv \pm 1$ so that $F + F \equiv \{0, \pm 2\}$. Adding ± 1 yields $F_{+3} \equiv \pm\{1, 3\}$ and again $F_{+4} \equiv \{0, \pm 2, \pm 4\}$, so that $F_{+3} \cup F_{+4}$ indeed cover all residues $\bmod 3^2$. Notice that F_{+3} and F_{+4} are disjoint which, although an exception, necessitates their union in the general statement of Theorem 3.2.

   It is conjectured that $F_{+3} \subseteq F_{+4}$ for $p > 6$, then $Z \equiv F_{+4}$ for primes $p > 6$.

2. For $p = 5$, again use analysis $\bmod p^2$, and test if $F(2A(h)+1)$ covers all nonzero $m5 \bmod 5^2$ (Lemma 3.2). Again $F = A \bmod p^2$, implying $A(h) \in F$. Now core $A \equiv F \equiv (2^5)^* \equiv \{7, -1, -7, 1\} \equiv \pm\{1, 7\}$, while $h \equiv 2$ with $A(2) \equiv 7$, or in base 5 code: $A(2) \equiv 12$ and $2A(h) + 1 \equiv 30$. Hence, $F(2A(h) + 1) \equiv \pm\{01, 12\}30 \equiv \pm\{30, 10\}$. This set indeed covers all four nonzero residues $m5 \bmod 5^2$.

4. CONCLUSIONS

The application of elementary semigroup concepts to structure analysis of residue arithmetic $\bmod p^k$ [2,3,6] is very useful, allowing divisors of zero. Fermat's inequality and Waring's representation are about powersums, thus about additive properties of closures in $Z(.) \bmod p^k$.

Fermat's inequality, viewed as anticlosure, reveals n^p as a powerful set of additive generators of $Z(+)$. Now $Z(.)$ has idempotent 1, generating only itself, while 1 generates all of $Z(+)$ (Peano).

Similarly, expanding 1 to the subgroup $F \equiv \{n^p\}$ of p^{th} power residues in $Z(.) \bmod p^k$, of order $|F| = |G|/p$, yields a most efficient additive generator with: $F_{+3} \cup F_{+4} \equiv Z(+) \bmod p^k$ for any prime $p > 2$. This is compatible for $p = 2$ with the known result of each positive integer being the sum of at most four squares.

The concept of *critical precision* (base p) is very useful for linking integer symmetric properties to residue arithmetic $\bmod p^k$, and quadratic analysis $(\bmod p^3)$ for generative purposes such as primitive roots.

Finally, for $p = 2$, the most practical of primes: $p^2 - 1 = p + 1 = 3$ is in fact a semiprimitive root of $1 \bmod 2^k$ for $k \geq 3$ (Theorem 3.1: Note 4, [3]: Lemma 2) yielding a useful engineering result [7].

REFERENCES

1. E.T. Bell, *The Development of Mathematics*, pp. 304–306, McGraw-Hill, (1945).
2. N.F. Benschop, The semigroup of multiplication $\bmod p^k$, an extension of Fermat's Small Theorem, and its additive structure, *Semigroups and their Applications*, (July 1996).
3. N.F. Benschop, Fermat's Small and Last Theorem, and a new binary number code, Grenoble, (also available as `http://www.iae.nl/users/benschop/199706-1.dvi`), *Logic and Architecture Synthesis*, 133–140, (December 1996).
4. T.M. Apostol, *Introduction to Analytical Number Theory*, Theorems 10.4–10.6, Springer-Verlag, (1976).
5. G. Hardy and E. Wright, *An Introduction to the Theory of Numbers*, Chapter 8.3, Theorem 123, Oxford University Press, (1979).
6. S. Schwarz, The role of semigroups in the elementary theory of numbers, *Math. Slovaca* **31** (4), 369–395, (1981).
7. N.F. Benschop, Patent US-5923888 logarithmic multiplier (dual bases 2 and 3), (July 1999).
8. A. Clifford and G. Preston, The algebraic theory of semigroups, *AMS Survey #7* **1**, 130–135, (1961).