Acta Math. Univ. Comenianae
Vol. LXXIV, 2(2005), pp. 169–184

ADDITIVE STRUCTURE OF THE GROUP OF UNITS MOD p^k, WITH CORE AND CARRY CONCEPTS FOR EXTENSION TO INTEGERS

N. F. BENSCHOP

Abstract. The additive structure of multiplicative semigroup $Z_{p^k} = Z(\cdot) \bmod p^k$ is analysed for prime $p > 2$. Order $(p-1)p^{k-1}$ of cyclic group G_k of units mod p^k implies product $G_k \equiv A_k B_k$, with cyclic 'core' A_k of order $p-1$ so $n^p \equiv n$ for core elements, and 'extension subgroup' B_k of order p^{k-1} consisting of all units $n \equiv 1 \bmod p$, generated by $p+1$. The p-th power residues $n^p \bmod p^k$ in G_k form an order $|G_k|/p$ subgroup F_k, with $|F_k|/|A_k| = p^{k-2}$, so F_k properly contains core A_k for $k \geq 3$.

The additive structure of subgroups A_k, F_k and G_k is derived by successor function $S(n) = n+1$, and by considering the two arithmetic symmetries $C(n) = -n$ and $I(n) = n^{-1}$ as functions, with commuting $IC = CI$, where S does not commute with I nor C. The four distinct compositions *SCI, CIS, CSI, ISC* all have period 3 upon iteration. This yields a *triplet* structure in G_k of three inverse pairs $(n_i,\ n_i^{-1})$ with $n_i + 1 \equiv -(n_{i+1})^{-1}$ for $i = 0, 1, 2$ where $n_0 \cdot n_1 \cdot n_2 \equiv 1 \bmod p^k$, generalizing the cubic root solution $n + 1 \equiv -n^{-1} \equiv -n^2 \bmod p^k$ $(p \equiv 1 \bmod 6)$.

Any solution *in core*: $(x+y)^p \equiv x + y \equiv x^p + y^p \mod p^{k>1}$ has exponent p distributing over a sum, shown to imply the known FLT inequality for integers. In such equivalence $\bmod p^k$ (FLT $case_1$) the three terms can be interpreted as naturals $n < p^k$, so $n^p < p^{kp}$, and the $(p-1)k$ produced carries cause FLT inequality. In fact, inequivalence mod p^{3k+1} is derived for the cubic roots of 1 mod $p^k (p \equiv 1 \bmod 6)$.

Introduction

The commutative semigroup $Z_{p^k}(\cdot)$ of multiplication mod p^k (prime $p>2$) has for all $k > 0$ just two idempotents: $1^2 \equiv 1$ and $0^2 \equiv 0$, and is the disjoint union of the corresponding maximal subsemigroups (Archimedian components [**4**], [**8**]). Namely the group G_k of units ($n^i \equiv 1 \bmod p^k$ for some $i > 0$) which are all relative prime to p, and maximal ideal N_k as nilpotent subsemigroup of all p^{k-1} multiples of p ($n^i \equiv 0 \bmod p^k$ for some $i > 0$). Notice that, since the analysis holds for any odd prime p, the index p in G_k and N_k is omitted for brevity of notation. Order $|G_k| = (p-1)p^{k-1}$ has two coprime factors, so that $G_k \equiv A_k B_k$, with 'core' A_k

Received June 17, 2003.
2000 *Mathematics Subject Classification.* Primary 11D41, 11P99, 11A15.
Key words and phrases. Residue arithmetic, ring, group of units, multiplicative semigroup, additive structure, triplet, cubic roots of unity, carry, Hensel, Fermat, FST, FLT.

and 'extension group' B_k of orders $p-1$ and p^{k-1} respectively. Residues of n^p form a subgroup $F_k \subset G_k$ of order $|F_k| = |G_k|/p$, to be analysed for its additive structure. Each $n \in A_k$ has $n^p \equiv n \bmod p^k$ denoted as FST_k , since this is related to Fermat's Small Theorem where $k = 1$.

Notation: Base p number representation is used, which is useful for computer experiments, as reported in Tables 1 and 2. This models residue arithmetic $\bmod p^k$ by considering only the k less significant digits, and ignoring the more significant digits. Congruence class $[n] \bmod p^k$ is represented by natural number $n < p^k$, encoded by k digits (base p). Class $[n]$ consists of all integers with the same least significant k digits as n. As usual, concatenation of operands indicates multiplication.

Define the *0-extension* of residue $n \bmod p^k$ as the natural number $n < p^k$ with the same k-digit representation (base p), and all more significant digits (at p^m, $m \geq k$) set to 0.

Signed residue $-n$ is only a convenient notation for the complement $p^k - n$ of n, which are both positive. $C[n]$ is a cyclic group of order n, such as $Z_{p^k}(+) \cong C[p^k]$. Units $\bmod p$ form a cyclic group $G_1 = C[p-1]$, and G_k of order $(p-1)p^{k-1}$ is also cyclic for $k > 1$ [**1**]. Finite *semigroup structure* is applied, and *digit analysis* of prime-base residue arithmetic, to study the combination of $(+)$ and $(\cdot) \bmod p^k$, especially the additive properties of multiplicative subgroups of ring $Z_{p^k}(+, \cdot)$

Elementary residue arithmetic, cyclic groups, and (associative) function composition will be used, starting at the known cyclic (one generator) nature [**1**] of the group G_k of units $\bmod p^k$. The direct product structure of G_k (Lemma 1.1 and Corollary 1.2) on the p^{k-2} extensions of $n^p \bmod p^2$ to cover all p-th power residues $\bmod p^k$ for $k > 2$ are known, but they are derived for completeness. Results beyond Section 1 are believed to be new.

The two symmetries of residue arithmetic $\bmod p^k$, defined as automorphisms of order 2, are complement $-n$ under $(+)$ and inverse n^{-1} under $(\cdot)$. Their role as functions $C(n) = -n$ and $I(n) = n^{-1}$, in the *triplet* additive structure of $Z(\cdot)$ $\bmod p^k$ (Lemma 3.1 and Theorem 3.1) is essential.

Symbols	and **Definitions** (odd prime p)
$Z_{p^k}(.)$	multiplicative semigroup $\bmod p^k$ (k-digit arithmetic base p)
$C[m]$	cyclic group of order m: e.g. $Z_{p^k}(+) \cong C[p^k]$
$x \in Z_{p^k}(.)$	unique product $x = g^i\ p^{k-j} \bmod p^k$ ($g^i \in G_j$ coprime to p)
0-extension X	of residue $x \bmod p^k$: the smallest non-negative integer $X \equiv x \bmod p^k$
(finite) extension U	of $x \bmod p^k$: any integer $U \equiv x \bmod p^k$
$G_k \equiv A_k \cdot B_k$	group of units n: $n^i \equiv 1 \bmod p^k$ (some $i > 0$), $\lvert G_k\rvert \equiv (p-1)p^{k-1}$
A_k	*core* of G_k, $\lvert A_k\rvert = p-1$ ($n^p \equiv n \bmod p^k$ for $n \in A_k$)
$B_k \equiv (p+1)^*$	extension group of all $n \equiv 1 \bmod p$, $\lvert B_k\rvert = p^{k-1}$
F_k	subgroup of all p-th power residues in G_k, $\lvert F_k\rvert = \lvert G_k\rvert/p$
$A_k \subset F_k \subset G_k$	proper inclusions only for $k \geq 3$ ($A_2 \equiv F_2 \subset G_2$)

Symbols	and **Definitions** (odd prime p)
$d(n)$	core increment $A(n+1)-A(n)$ of core func'n $A(n) \equiv n^q$, $q=\|B_k\|$
FST_k	core A_k ($p-1$ residues) extends FST ($n^p \equiv n \bmod p$) to mod $p^{k>1}$
solution in core	$x^p+y^p \equiv z^p \mod p^k$ with x,y,z in core A_k.
period of $n \in G_k$	order $\|n^*\|$ of subgroup generated by n in $G_k(\cdot)$
normation	divide $x^p+y^p \equiv z^p \mod p^k$ by one term (in F_k) to yield one term ± 1
complement $-n$	unique in $Z_{p^k}(+)$: $-n+n \equiv 0 \mod p^k$
inverse n^{-1}	unique in $G_k(\cdot)$: $n^{-1} \cdot n \equiv 1 \mod p^k$
1-complement pair	pair $\{m,n\}$ in $Z_{p^k}(+)$: $m+n \equiv -1 \mod p^k$
inverse-pair	pair $\{a,a^{-1}\}$ of inverses in G_k
triplet	3 inv. pairs: $a+b^{-1} \equiv b+c^{-1} \equiv c+a^{-1} \equiv -1$, ($abc \equiv 1 \bmod p^k$)
triplet^p	a triplet of p-th power residues in subgroup F_k
symmetry mod p^k	$-n$ and n^{-1}: order 2 automorphism of $Z_{p^k}(+)$ resp. $G_k(\cdot)$
EDS property	Exponent Distributes over a Sum: $(a+b)^p \equiv a^p+b^p \mod p^k$

1. Structure of the group G_k of units

Lemma 1.1. *$G_k \cong A'_k \times B'_k \cong C[p-1] \cdot C[p^{k-1}]$ and $Z(\cdot)$ mod p^k has a sub-semigroup isomorphic to $Z(\cdot)$ mod p.*

Proof. Cyclic group G_k of *units* n ($n^i \equiv 1$ for some $i>0$) has order $(p-1)p^{k-1}$, namely p^k minus p^{k-1} multiples of p. Then $G_k = A'_k \times B'_k$, the direct product of two relative prime cycles, with corresponding subgroups A_k and B_k, so that $G_k \equiv A_k\ B_k$ where:
extension group $B_k = C[\ p^{k-1}\ ]$ consists of all p^{k-1} residues mod p^k that are 1 mod p, and
core $A_k = C[p-1]$, so $Z_{p^k}(\cdot)$ contains sub-semigroup $A_k \cup 0 \cong Z_p(\cdot)$ □

Core A_k, as $p-1$ cycle mod p^k, is Fermat's Small Theorem $n^p \equiv n \bmod p$ extended to $k>1$ for p residues (including 0), to be denoted as FST_k.
Recall that $n^{p-1} \equiv 1 \bmod p$ for $n \not\equiv 0 \bmod p$ (FST), then Lemma 1.1 implies:

Corollary 1.1. *With $|B| = p^{k-1} = q$ and $|A| = p-1$, core $A_k = \{n^q\}$ mod p^k ($n = 1, \ldots, p-1$) extends FST for $k>1$, and $B_k = \{n^{p-1}\}$ mod p^k consists of all p^{k-1} residues* 1 mod p *in G_k.*

Subgroup $F_k \equiv \{n^p\}$ mod p^k of all p-th power residues in G_k, with $F_k \supseteq A_k$ (only $F_2 \equiv A_2$) and order $|F_k| = |G_k|/p = (p-1)p^{k-2}$, consists of *all* p^{k-2} extensions mod p^k of the $p-1$ p-th power residues in G_2, which has order $(p-1)p$. Consequently:

Corollary 1.2. *Each extension of n^p mod p^2 (in F_2) is a p-th power residue (in F_k).*

Core generation: The $p-1$ residues $n^q \bmod p^k$ ($q = p^{k-1}$) define core A_k for $0< n < p$. Cores A_k for successive k are produced as the p-th power of each $n_0 < p$ recursively

$$(n_0)^p \equiv n_1,\ (n_1)^p \equiv n_2,\ (n_2)^p \equiv n_3,\ \ldots$$

where n_i has $i+1$ digits (base p). In more detail:

Lemma 1.2. *For non-negative digits $a_i < p$ the $p-1$ naturals $a_0 < p$ define core*

$$A_k(a_0) \equiv (a_0)^{p^{k-1}} \equiv a_0 + \sum_{i=1}^{k-1} a_i p^i \mod p^k,$$

and

$$A_{k+1}(a_0) \equiv [\ A_k(a_0)\ ]^p \mod p^{k+1}.$$

Proof. Let $a = a_0 + mp < p^2$ be in core A_2, so $a^p \equiv a \bmod p^2$. Then

$$a^p = (mp + a_0)^p \equiv a_0^{p-1} mp^2 + a_0^p \equiv mp^2 + a_0^p \mod p^3,$$

by FST. Core digit a_1 of weight p is not found in this way as function of a_0, requiring actual computation, except for $a \equiv p \pm 1$ as in (1) and (1′). It depends on the *carries* produced in computing the p-th power of a_0. Similarly, the *next* more significant digit in core $A_{k+1}(n)$ is found by computing, with k+1 digit precision, the p-th power a^p of 0-extension $a < p^k$ in core A_k, leaving core A_k fixed, because $a^p \equiv a \bmod p^k$. □

Notice $(p^2 \pm 1)^p \equiv p^3 \pm 1 \bmod p^5$, and $(p+1)^p \equiv p^2 + 1 \bmod p^3$ yields by induction on m:

(1) $$(p+1)^{p^m} \equiv p^{m+1} + 1 \mod p^{m+2}$$

(1′) $$(p-1)^{p^m} \equiv p^{m+1} - 1 \mod p^{m+2}$$

Lemma 1.3. *Extension group B_k is generated by $p+1 \bmod p^k$, with $|B_k| = p^{k-1}$, and each subgroup $S \subseteq B_k$, $|S| = |B_k|/p^s$ has sum*

$$\sum S \equiv |S| \mod p^k \not\equiv 0 \mod p^k.$$

Proof. For the smallest x with $(p+1)^x \equiv 1 \bmod p^k$, the *period* of $p+1$, (1) implies $m+1 = k$. So $m = k-1$, thus period p^{k-1}. No smaller x generates $1 \bmod p^k$ since $|B_k|$ has only divisors p^s.

B_k consists of all p^{k-1} residues which are $1 \bmod p$. The order of each subgroup $S \subset B_k$ must divide $|B_k|$, so that $|S| = |B_k|/p^s$ ($0 \le s < k$) and $S = \{1 + m \cdot p^{s+1}\}$ ($m = 0, \ldots, |S|-1$). Then $\sum S = |S| + p^{s+1} \cdot |S|(|S|-1)/2 \bmod p^k$, where $p^{s+1} \cdot |S| = p \cdot |B_k| = p^k$, so that $\sum S = |S| = p^{k-1-s} \bmod p^k$. Hence no subgroup of B_k sums to $0 \bmod p^k$. □

Corollary 1.3. *For core $A_k \equiv g^*$, each unit $n \in G_k \equiv A_k B_k$ has the form:*

$$n \equiv g^i (p+1)^j \mod p^k$$

for a unique pair of non-negative exponents $i < |A_k|$ and $j < |B_k|$.

Pair (i, j) are the exponents in the core- and extension- component of unit n. In case $p = 2$, the most interesting prime for computer engineering purposes, the next binary number representation is readily verified [**3**], [**7**]:

Lemma 1.4. *For $p = 2$: $p + 1 = 3$ is a semi-primitive root of* $1 \bmod 2^k$ *for $k > 2$.*

In other words, for base $p = 2$ and precision $k > 2$: each odd residue mod 2^k is a unique signed power of 3. Hence an efficient k-bit binary number code is

$$n = \pm 3^i \cdot 2^j \mod 2^k,$$

for all integers $0 \le n < 2^k$, with unique non-negative index pair $i < 2^{k-2}$ and $j \le k$.

Clearly, this allows a dual-base (2, 3) binary logarithmetic code, which reduces multiplication to addition of the two indices, and XOR (add mod 2) of the involved signs (see US-patent [**7**]).

Theorem 1.1. *Each subgroup $S \supset 1$ of core A_k sums to* $0 \mod p^k$ *$(k > 0)$.*

Proof. For *even* $|S|$: -1 in S implies pairwise zero-sums. In general: $c \cdot S = S$ for all c in S, and $c \sum S = \sum S$, so $S \cdot x = x$, writing x for $\sum S$. Now for any g in G_k: $|S \cdot g| = |S|$ so that $|S \cdot x|$=1 implies x not in G_k, hence $x = g \cdot p^e$ for some g in G_k and $0 < e < k$ or $x = 0$ $(e = k)$. Then $S \cdot x = S(g \cdot p^e) = (S \cdot g)p^e$ with $|S \cdot g| = |S|$ if $e < k$. So $|S \cdot x|$=1 yields e=k and $x = \sum S$=0. □

Consider the normation of an additive equivalence $a + b \equiv c \bmod p^k$ in units group G_k, by multiplying all terms with the inverse of one of these terms, to yield rhs -1 as right hand side:

(2) 1-complement form: $a + b \equiv -1 \mod p^k$ in G_k,

(digitwise sum $p - 1$, no carry).

For instance the well known p-th power residue equivalence: $x^p + y^p \equiv z^p$ in F_k yields:

(2′) normal form: $a^p + b^p \equiv -1 \mod p^k$ in G_k,

with a special case in core A_k, considered next.

2. The cubic root solution in core, and core symmetries

Lemma 2.1. *Cubic roots* $a^3 \equiv 1 \bmod p^k$ *$(p \equiv 1 \bmod 6,\ k > 1)$ are p-th power residues in core A_k, and* $a + a^{-1} \equiv -1 \bmod p^k$ *$(a \not\equiv -1)$ has no corresponding integers as p-th powers $< p^{kp}$.*

Proof. If $p \equiv 1 \bmod 6$ then 3 divides $p - 1$, implying a core subgroup $S = \{a, a^2, 1\}$ of three p-th powers: the cubic roots $a^3 \equiv 1$ in G_k, with sum 0 mod p^k (Theorem 1.1). Now $a^3 - 1 = (a-1)(a^2+a+1)$, so for $a \ne 1 :\ a^2+a+1 \equiv 0$, hence $a + a^{-1} \equiv -1$ solves the normed (2′), being a *root-pair* of inverses with $a^2 \equiv a^{-1}$. Subgroup $S \subset A_k$ consists of p-th power residues with $n^p \equiv n \bmod p^k$.

Core $A = (43)^* = 43\ 42\ 66\ 24\ 25\ 01 \pmod{7^2}$

Cubic rootpair: $42 + 24 \equiv 66 \equiv -1$

$42 + 1 \equiv -(42)^{-1}$

$-a^{-1} \equiv a + 1$

Complement $C(n) = -n$
Inverse $I(n) = n^{-1}$
Succesor $S(n) = n + 1$

$42^3 \equiv 1 \mod 7^2$

Symmetries:
$-n$ (diagonal) C
n^{-1} (vertical) I
$-n^{-1}$ (horizontal) IC=CI

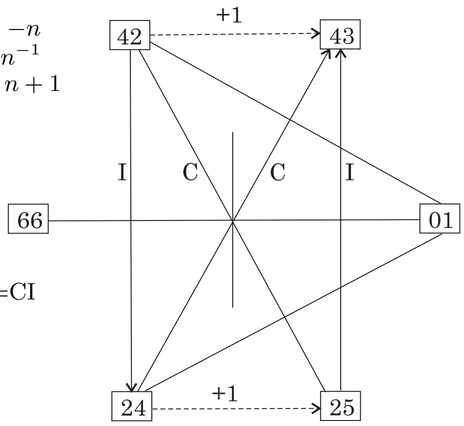

Figure 1. Core A_2 mod 7^2 (6-cycle), Cubic roots {42, 24, 01} (3-cycle) in core.

Write b for a^{-1}, then $a^p + b^p \equiv -1$ and $a + b \equiv -1$, hence $a^p + b^p \equiv (a+b)^p$ mod p^k. The "exponent p distributes over a sum" (EDS) property implies $A^p + B^p < (A+B)^p$ for the corresponding 0-extensions $A,\ B,\ A+B$ of residues $a,\ b,\ a+b$ mod p^k. □

1. Successive powers g^i of generator g of G_k produce $|G_k|$ points (k-digit residues) counter clockwise on a unit circle (Figures 1, 2). Inverse pairs $(a,\ a^{-1})$ are connected *vertically*, complements $(a,\ -a)$ *diagonally*, and pairs $(a,\ -a^{-1})$ *horizontally*, representing functions $I,\ C$ and $IC = CI$ respectively (Theorem 3.1).
2. Scaling any equation, such as $a + 1 \equiv -b^{-1}$, by a factor $s \equiv g^i \in G_k \equiv g^*$, yields $s(a+1) \equiv -s/b$ mod p^k, represented by a rotation counter clockwise over i positions.

2.1. Another derivation of the cubic roots of 1 mod p^k

The cubic root solution was derived, for 3 dividing $p - 1$, via subgroup $S \subset A_k$ of order 3 (Theorem 1.1). For completeness a derivation using elementary arithmetic follows.

Notice $a + b \equiv -1$ to yield $a^2 + b^2 \equiv (a+b)^2 - 2ab \equiv 1 - 2ab$, and:

$$a^3 + b^3 \equiv (a+b)^3 - 3(a+b)ab \equiv -1 + 3ab.$$

The combined sum is $ab - 1$:

$$\sum_{i=1}^{3}(a^i + b^i) \equiv \sum_{i=1}^{3} a^i + \sum_{i=1}^{3} b^i \equiv ab - 1 \mod p^k.$$

Find a, b for $ab \equiv 1 \mod p^k$. Now

$$n^2 + n + 1 = (n^3 - 1)/(n - 1) = 0 \quad \text{for} \quad n^3 \equiv 1 \quad (n \neq 1),$$

hence $ab \equiv 1 \mod p^k$, $(k > 0)$ if $a^3 \equiv b^3 \equiv 1 \mod p^k$, with 3 dividing $p-1$ ($p \equiv 1 \mod 6$). Cubic roots $a^3 \equiv 1 \mod p^k$ exist for any prime $p \equiv 1 \mod 6$ at any precision $k > 0$.

In the next section other solutions of $\sum_{i=1}^{3} a^i + \sum_{i=1}^{3} b^i \equiv 0 \mod p^k$ will be shown, depending not only on p but also on k, with $ab \equiv 1 \mod p^2$ but $ab \not\equiv 1 \mod p^3$, for some primes $p \geq 59$.

2.2. Core increment symmetry mod p^{2k+1} and asymmetry mod p^{3k+1}

Consider:
core function $A_k(n) = n^q$ ($q = |B_k| = p^{k-1}$) as natural monomial,
core increment $d_k(n) = A_k(n+1) - A_k(n) = (n+1)^q - n^q$ (even degree $q-1$),
natural core $C_k(n) < p^k$ with $A_k(n) \equiv C_k(n) \mod p^k$,
integer core increment $D_{k+1}(n) = [C_k(n+1)]^p - [C_k(n)]^p$, with absolute value less than p^{kp}.

Recall: for natural $n < p$ the p-th power residues $[A_k(n)]^p \mod p^{k+1}$ form core A_{k+1} (Lemma 1.2). For any core element $a \in C_k$: $a^{p-1} \equiv 1 \mod p^k$. By FST: $C_k(n) \equiv n \mod p$, so $D_k(n) \equiv 1 \mod p$, and $D_k(n)$ is called *core increment*, although in general $D_k(n) \not\equiv 1 \mod p^k$ for $k > 2$. Core naturals $C_k(n) < p^k$ are considered in order to study natural p-th power sums.

For example consider $p = 7$ (Figure 1). The cubic roots in core A_2 are $\{42,\ 24,\ 01\} \mod 7^2$, with 7-th powers $\{642,\ 024,\ 001\}$ in core A_3. In full 14 digits (base 7):

$$42^7 + 24^7 = 0\ 14\ 24\ 06\ 25\ 00\ 66\ 6\ (k{=}2) \quad \text{versus} \quad 66^7 = 6\ 02\ 62\ 04\ 64\ 00\ 66\ 6$$

which are equivalent mod $7^{2k+1} = 7^5$, but differ mod 7^6 hence also mod $7^{3\cdot 2+1} = 7^7$. Cubic roots $\{3642,\ 3024\}$ in core A_4, as 7-th powers of cubic roots in A_3 (k=3), have increment 1 mod 7^7 with increment symmetry mod $7^{2k+1} = 7^7$, and asymmetry mod $p^{3k+1} = 7^{10}$. See also Table 1. This core- and carry effect is generalized for integers as follows.

Lemma 2.2 (Core increment symmetry and asymmetry). *For $q = |B_k| = p^{k-1}$ ($k \geq 1$) and natural m, $n < p$:*

(a) *Core residues $A_k(n) \equiv n^q \mod p^k$ and increments $d_k(n) \equiv A_k(n+1) - A_k(n) \mod p^k$ have period p in n.*

(b) *If $m + n = p$ then $A_k(p-n) \equiv A_k(-n) \equiv -A_k(n) \mod p^k$* (odd symm.).

(c) *If $m + n = p - 1$ then $D_{k+1}(m) \equiv D_{k+1}(n) \mod p^{2k+1}$* (even symm.).

(d) *If $m + n = p - 1$ and natural cubic roots $C_k(m) + C_k(n) = p^k - 1$ then $D_{k+1}(m) \not\equiv D_{k+1}(n) \mod p^{3k+1}$* (asymmetry)

Proof. (a) Core function $A_k(n) \equiv n^q \mod p^k$ ($q = p^{k-1}$, $n \not\equiv 0 \mod p$) has just $p-1$ distinct residues with $(n^q)^p \equiv n^q \mod p^k$, and $A_k(n) \equiv n \mod p$ (FST). Include non-core $A_k(0) \equiv 0$ then $A_k(n) \mod p^k$ is periodic in n with period p, so $A_k(n+p) \equiv A_k(n) \mod p^k$. Hence difference $d_k(n) \mod p^k$ of two functions of period p also has period p.

```
n      core C_k      core C_[k+1]==(C_k)^p   Core_incr.      p=7 (base 7)
          C_1      v         C_2     v v                <---- mod p^3
 1.  0 0 0 0 0 0 0 1    0 0 0 0 0 0 0 1    0 0 0 0 0 2 4 1
 2.  0 0 0 0 0 0 0 2    0 0 0 0 0 2 4 2    0 0 0 0 6.0 0 1  /\
 3.  0 0 0 0 0 0 0 3    0 0 0 0 6 2 4 3    0 0 0 5 6 2 5 1 sym
 4.  0 0 0 0 0 0 0 4    0 0 0 6 5 5 2 4    0 0 3 4 5.0 0 1  \/
 5.  0 0 0 0 0 0 0 5    0 0 4 4 3 5 2 5    0 1 5 0 0 2 4 1
 6.  0 0 0 0 0 0 0 6    0 2 2 4 4 0 6 6    6 4 4 2 2 6 0 1

          C_2    v v       C_3     v v v         <-------- mod p^5
 1.  0 0 0 0 0 0 0 1    0 0 0 0 0 0 0 1    4 6 6 3 4 6 4 1
 2.  0 0 0 0 0 0 4 2    4 6 6 3 4 6 4 2    5 4 3.0 0 0 0 1  /\
 3.  0 0 0 0 0 0 4 3    3 4 2 3 4 6 4 3    4 5 2 6 5 0 5 1 sym
 4.  0 0 0 0 0 0 2 4    1 2 5 3 3 0 2 4    6 0 0.0 0 0 0 1  \/
 5.  0 0 0 0 0 0 2 5    0 2 5 3 3 0 2 5    4 3 5 3 4 6 4 1
 6.  0 0 0 0 0 0 6 6    4 6 4 0 0 6 6 6    2 0 2 6 6 0 0 1

          C_3  v v v       C_4   v v v v     <------------ mod p^7
 1.  0 0 0 0 0 0 0 1    0 0 0 0 0 0 0 1    6 4 1 4 3 6 4 1
 2.  0 0 0 0 0 6 4 2    6 4 1 4 3 6 4 2 136.0 0 0 0 0 0 1  /\
 3.  0 0 0 0 0 6 4 3    5 4 1 4 3 6 4 3    2 5 3 5 6 0 5 1 sym
 4.  0 0 0 0 0 0 2 4    1 2 5 3 3 0 2 4 666.0 0 0 0 0 0 1  \/
 5.  0 0 0 0 0 0 2 5    0 2 5 3 3 0 2 5    3 4 1 4 3 6 4 1
 6.  0 0 0 0 0 6 6 6    4 0 0 0 6 6 6 6    2 6 6 6 0 0 0 1
```

Table 1. Cores $C_1..C_3$, increment symmetry mod $p^{[2k+1]}$ of $C_2..C_4$. For cubic roots of 1 mod p^k: asymmetry mod $p^{[3k+1]}$ in $C_2..C_4$..

(b) $(-n)^q = -n^q$, odd $q = p^{k-1}$, yields *odd symmetry*

$$A_k(p-n) \equiv A_k(-n) \equiv -A_k(n) \mod p^k$$

(c) Difference polynomial $d_k(n)$ has leading term $q\ n^{q-1}$. Even degree $q-1$ results in *even symmetry*

$$d_k(n-1) = n^q - (n-1)^q = -(-n)^q + (-n+1)^q = d_k(-n).$$

Now $C_k(n) = p^k - C_k(p-n) < p^k$, hence for $m+n = p-1$, $C_k(m+1) = p^k - C_k(n)$, so

$$D_{k+1}(m) = [p^k - C_k(n)]^p - [C_k(m)]^p \quad \text{and} \quad D_{k+1}(n) = [p^k - C_k(m)]^p - [C_k(n)]^p.$$

Briefly denote naturals $C_k(m) = a$, $C_k(n) = b$, and $h = (p-1)/2$ then

$$\begin{aligned} D_{k+1}(m) - D_{k+1}(n) &= [(p^k - b)^p + b^p] - [(p^k - a)^p + a^p] \\ (*) \qquad &\equiv -h[\ b^{p-2} - a^{p-2}\ ]\ p^{2k+1} + [\ b^{p-1} - a^{p-1}\ ]\ p^{k+1} \mod p^{3k+1} \\ &\equiv\ 0 \mod p^{2k+1}, \end{aligned}$$

because by FST: $a^{p-1} \equiv\ b^{p-1} \equiv 1 \bmod p^k$.

(d) Carry difference $(b^{p-1} - a^{p-1})/p^k \not\equiv h(b^{p-2} - a^{p-2}) \bmod p^k$ is required, to avoid cancellation in (*). It suffices to show this for $k = 1$ and 0-extensions $1 < a, b < p$ of cubic roots of 1 mod p. Using $b \equiv a^2 \equiv a^{-1}$, $b^{p-2} - a^{p-2} \equiv -(b-a)$ mod p , and $h = (p-1)/2 \equiv -1/2 \bmod p$ the *carry difference* must satisfy (cd)

$$\text{(cd)} \qquad \frac{(b^{p-1} - a^{p-1})}{p} \not\equiv \frac{(b-a)}{2} \mod p.$$

Let $a^3 \equiv cp+1 \mod p^2$ with some carry c, then for $m>0$: $a^{3m} \equiv mcp+1 \mod p^2$. So $a^{p-1} \equiv [(p-1)/3]cp+1 \mod p^2$, and similarly for cubic root power b^3. In other words, in extension group $B_2 \equiv \{xp+1\} \equiv (p+1)^x \mod p^2$ the coefficient of p is proportional to the exponent. For a^{p-1} versus a^3 the ratio is $(p-1)/3$. However in (cd), adapted for third powers a^3, b^3 it is $(p-1)/(3/2) = 2(p-1)/3$, hence the (cd) inequivalence holds.

So for the cubic roots of 1 mod p^k, with $a+b = C_k(m)+C_k(n) = p^k-1$ core increment has asymmetry

$$D_{k+1}(m) \not\equiv D_{k+1}(n) \mod p^{3k+1}. \qquad \square$$

Corollary 2.1. *Let prime $p \equiv 1 \bmod 6$, and any precision $k>0$. For $x^3 \equiv y^3 \equiv 1 \mod p^k$ (cubic roots $x,y \not\equiv 1$) 0-extensions $X,Y<p^k$ of x,y have $X^p,Y^p \mod p^{k+1}$ in core A_{k+1} with $X^p+Y^p \equiv -1 \mod p^{k+1}$ and $X^p+Y^p \not\equiv (p^k-1)^p \mod p^{3k+1}$.*

3. Symmetries as functions yield 'triplets'

Any solution of (2'): $a^p+b^p=-1 \mod p^k$ has at least one term (-1) in core, and at most all three terms in core A_k. To characterize such solution by the number of terms in core A_k, quadratic analysis (mod p^3) is essential since proper inclusion $A_k \subset F_k$ requires $k \geq 3$. The cubic root solution, involving one inverse pair (Lemma 2.1) has all three terms in core A_k $(k>1)$. However, a computer search (Table 2) reveals another type of solution of (2') mod p^2 for some $p \geq 59$, namely three inverse pairs of p-th power residues, denoted triplet^p, in core A_2.

Lemma 3.1. *A triplet^p of three inverse-pairs of p-th power residues in F_k satisfies*

(3a) $a+b^{-1} \equiv -1 \mod p^k$
(3b) $b+c^{-1} \equiv -1 \mod p^k$
(3c) $c+a^{-1} \equiv -1 \mod p^k$ *with* $abc \equiv 1 \mod p^k$.

Proof. Multiplying by b, c, a resp. maps (3a) to (3b) if $ab \equiv c^{-1}$, and (3b) to (3c) if $bc \equiv a^{-1}$, and (3c) to (3a) if $ac \equiv b^{-1}$. All three conditions imply $abc \equiv 1 \mod p^k$. $\square$

Table 2 shows all normed solutions of $(2')$ mod p^2 for $p<200$, with a triplet^p at $p = 59, 79, 83, 179, 193$. The cubic roots, indicated by C_3, occur only at $p \equiv 1 \mod 6$, while a triplet^p can occur for either prime type $\pm 1 \mod 6$. More than one triplet^p can occur per prime: two at $p=59$, three at 1093 (dec) = [1111111] base 3 (one of the two known Wieferich primes [**9**], [**6**], and four at 36847, each the first occurrence of such multiple triplet^p). There are primes for which both root forms occur, e.g. $p=79$ has a cubic root solution as well as a triplet^p.

Such loop of inverse-pairs in residue ring $Z \mod p^k$ cannot have a length beyond 3, seen as follows. Consider the successor $S(n) = n+1$ and the two symmetries: complement $C(n) = -n$ and inverse $I(n) = n^{-1}$, as functions which compose associatively.

```
Find a+b = -1 mod p^2 (in A=F < G): Core A={n^p=n}, F={n^p} =A if k=2.
 G(p^2)=g*, log-code: log(a)=i, log(b)=j;  a.b=1 --> i+j=0 (mod p-1)

TRIPLET^p: a+ 1/b= b+ 1/c= c+ 1/a=-1; a.b.c=1; (p= 59 79 83 179 193 ...
^^^^^^

Root-Pair:  a+ 1/a=-1; a^3=1 ('C3') <--> p=6m+1 (Cubic rootpair of 1)
^^^^^^^^^

p:6m+-1 g=generator;   p < 2000:  two  triplets at p= 59, 701, 1811
  5:-   2                        three triplets at p= 1093
  7:+   3  C3    11:-  2
 13:+   2  C3    17:-  3
 19:+   2  C3    23:-  5   29:-   2
 31:+   3  C3
 37:+   2  C3    41:-  6
 43:+   3  C3    47:-  5
 53:-   2                    log    lin mod p^2
 59:-   2                  ------  ------------
   -2,-25( 40 15, 18 43)  25, 23( 35 11, 23 47) -23,  2( 53 54,  5  4)
              --      --              --      --              --     --
   27, 19( 18 44, 40 14) -19,  8( 13 38, 45 20)  -8,-27(  5  3, 53 55)
 61:+   2  C3
 67:+   2  C3    71:-  7
 73:+   5  C3
 79:+   3  C3
   30, 20( 40 46, 38 32) -20, 10( 36 42, 42 36) -10,-30( 77 11,  1 67)
 83:-   2
   21,  3(  9 74, 73  8)  -3, 18( 54 52, 28 30) -18,-21( 13 36, 69 46)
 89:-   3
 97:+   5  C3   101:-  2
103:+   5  C3   107:-  2
109:+   6  C3   113:-  3
127:+   3  C3   131:-  2   137:-  3
139:+   2  C3   149:-  2
151:+   6  C3
157:+   5  C3
163:+   2  C3   167:-  5   173:-  2
179:-   2
 19,  1( 78 176,100  2)  -1, 18( 64 90,114 88) -18,-19( 88 59, 90 119)
181:+   2  C3   191:- 19
193:+   5  C3
 -81, 58( 64 106,128 86) -58, 53( 4 101,188 91) -53, 81(188 70, 4 122)
197:-   2
199:+   3  C3
```

Table 2. FLT_2 root: inv-pair (C3) & triplet^p (for $p < 200$).

Theorem 3.1 (Two basic solution types)**.** *Each normed solution of* $(2')$ *is (an extension of) a triplet^p or an inverse- pair.*

Proof. Assume that r equations $1 - n_i^{-1} \equiv n_{i+1}$ form a loop of length r (indices mod r). Consider function $ICS(n) \equiv 1 - n^{-1}$, composed of the three elementary functions: Inverse, Complement and Successor, in that sequence. Let $E(n) \equiv n$ be the identity function, and $n \neq 0, 1, -1$ to prevent division by zero, then under function composition the third iteration $[ICS]_3 = E$, since $[ICS]_2(n) \equiv -1/(n-1) \rightarrow [ICS]_3(n) \equiv n$ (repeat substituting $1 - n^{-1}$ for n). Since C and I commute, IC=CI, the $3! = 6$ permutations of $\{I, C, S\}$ yield only four distinct dual-folded-successor *"dfs"* functions:

$$ICS(n) = -n^{-1}, \qquad SCI(n) = -(1+n)^{-1},$$
$$CSI(n) = (1-n)^{-1}, \quad ISC(n) = -(1+n^{-1}).$$

By inspection each of these has $[dfs]_3 = E$, referred to as *loop length* 3. For a cubic rootpair $dfs = E$, and 2-loops do not occur since there are no duplets (see Section 3.1 note 2). Hence solutions of (2′) have only *dfs* function loops of length 1 and 3: inverse pair and triplet^p. □

A special triplet^p occurs if one of a, b, c equals 1, say $a \equiv 1$. Then $bc \equiv 1$ since $abc \equiv 1$, while (3a) and (3c) yield $b^{-1} \equiv c \equiv -2$, so $b \equiv c^{-1} \equiv -2^{-1}$. Although triplet $(a, b, c) \equiv (1, -2, -2^{-1})$ satisfies conditions (3), 2 is not in core A_k $(k > 2)$, and by symmetry $a, b, c \not\equiv 1$ for any triplet^p of form (3).

If $2^p \not\equiv 2 \mod p^2$ then 2 is not a p-th power residue, so triplet $(1, -2, -2^{-1})$ is not a triplet^p for such primes, that is: at least all primes $p < 4 \cdot 10^{12}$ [**6**], except the two Wieferich primes [**9**]: 1093 (dec) = [1111111] base 3, and 3511 (dec) = [6667] base 8.

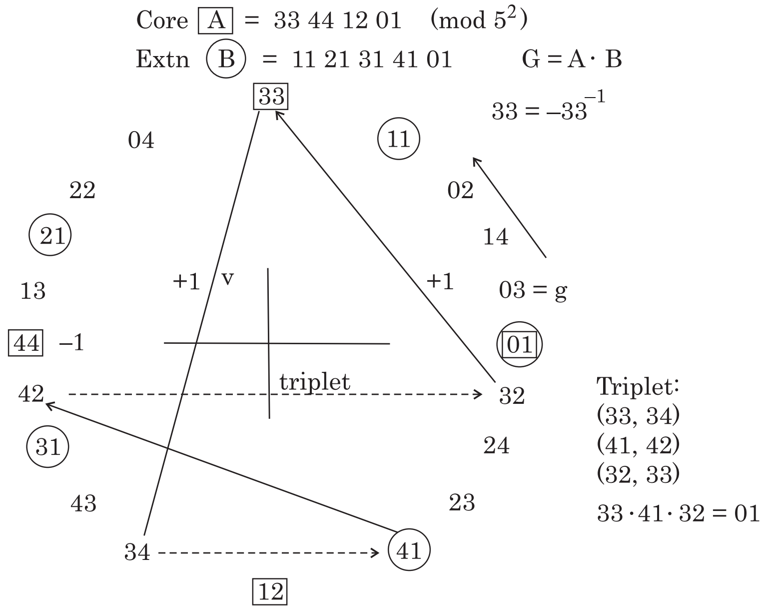

Figure 2. G = A · B = g^* (mod 5^2), Cycle in the plane.

3.1. A triplet for each unit n in G_k

Notice the proof of Theorem 3.1 does not require p-th power residues. So any $n \in G_k$ generates a triplet by iteration of one of the four *dfs* functions, yielding the main triplet structure of G_k

Corollary 3.1. *Each unit n in G_k $(k > 0)$ generates a triplet of three inverse pairs, except if $n^3 \equiv 1$ and $n \not\equiv 1 \mod p^k$ $(p \equiv 1 \mod 6)$, which involves one inverse pair.*

Starting at $n_0 \in G_k$ six triplet residues are generated upon iteration of e.g. $SCI(n)$: $n_{i+1} \equiv -(n_i+1)^{-1}$ (indices mod 3), or another *dfs* function to prevent a non-invertable residue. Less than 6 residues are involved if 3 or 4 divides $p-1$

If $3|(p-1)$ then a cubic root of 1 ($a^3 \equiv 1,\ a \not\equiv 1$) generates just 3 residues: $a+1 \equiv -a^{-1}$ – together with its complement this yields a subgroup $(a+1)^* \equiv C_6$ (Figure 1, $p=7$).

If 4 divides $p-1$ then an x on the vertical axis has $x^2 \equiv -1$ so $x \equiv -x^{-1}$, so the three inverse pairs involve then only five residues (Figure 2, $p=5$).

1. It is no coincidence that the period 3 of each *dfs* composition exceeds by one the number of symmetries of finite ring $Z(+,\ \cdot) \mod p^k$.
2. No duplet occurs: multiply $a+b^{-1} \equiv -1$, $b+a^{-1} \equiv -1$ by b resp. a. Then $ab+1 \equiv -b$ and $ab+1 \equiv -a$, so that $-b \equiv -a$ and $a \equiv b$.
3. Basic triplet mod 3^2: $G_2 \equiv 2^* \equiv \{2,4,8,7,5,1\}$ is a 6-cycle of residues mod 9. Iterate $SCI(1)^* : -(1+1)^{-1} \equiv 4,\ -(4+1)^{-1} \equiv 7,\ -(7+1)^{-1} \equiv 1$, and $abc \equiv 1 \cdot 4 \cdot 7 \equiv 1$ mod 9.

3.2. The EDS argument extended to non-core triplets

The EDS argument for the cubic root solution CR (Lemma 2.1), with all three terms in core, also holds for any triplet^p mod p^2. Because $A_2 \equiv F_2 \mod p^2$, so all three terms are in core for some linear transform (5). Then for each of the three equivalences (3a) – (3c) holds the EDS property: $(x+y)^p \equiv x^p + y^p$, and thus no finite (equality preserving) extension exists, yielding inequality for the corresponding integers for all $k>1$, to be shown next. A cubic root solution is a special triplet^p for $p \equiv 1 \mod 6$, with $a \equiv b \equiv c$ in (3a) – (3c).

Denote the $p-1$ core elements as residues of integer function $A_k(n) = n^{|B_k|}$ ($0<n<p$), then for any $k>2$ consider core increment form:

$$(4) \qquad A_k(n+1) - A_k(n) \equiv (r_n)^p \mod p^k, \quad \text{where} \quad (r_n)^p \equiv 1 \mod p^2.$$

This triplet^p rootform with two terms in core, and $(r_n)^p \not\equiv 1 \mod p^3$, is useful for the additive analysis of subgroup F_k of p-th power residues mod p^k, in essence: the known Fermat's Last Theorem FLT case$_1$ for residues coprime to p, discussed in the next section.

Any assumed FLT case$_1$ solution (5) for integers less than p^{kp} can be transformed to (4), in two equality preserving steps. Namely first a multiplicative scaling by an integer p-th power factor s^p that is 1 mod p^2 (so $s \equiv 1 \mod p$), to yield as one lefthand term the core residue $A_k(n+1) \mod p^k$. And secondly an additive translation by integer term t which is 0 mod p^2 applied to both sides, resulting in the other lefthand term $-A_k(n) \mod p^k$, while preserving integer equality. Assuming, without loss, the normed form with $z^p \equiv 1 \mod p^2$, such linear transformation (s,t) yields:

$$(5) \qquad x^p + y^p = z^p \longleftrightarrow (sx)^p + (sy)^p + t = (sz)^p + t \quad \text{[integers]},$$

with $s^p \equiv A_k(n+1)/x^p$, $\ (sy)^p + t \equiv -A_k(n) \mod p^k$, so:

$$(5') \qquad A_k(n+1) - A_k(n) \equiv (sz)^p + t \mod p^k, \quad \text{equivalent to } 1 \mod p^2.$$

With $s^p \equiv z^p \equiv 1$, $t \equiv 0 \mod p^2$ this yields an equivalence which is $1 \mod p^2$, hence a p-th power residue, and $(5')$ has two of the three terms in core, for $k > 2$. All three terms of a triplet^p mod p^2 are in core (Corrolary 1.2). In core increment form (4) for $k > 2$ this holds apparently only if the righthand side $(r_n)^p \equiv 1 \mod p^k$, yielding:

Corollary 3.2 (For precision $k > 2$ (base p)). *Core increment form* (4) *with all three terms in core A_k is the cubic root solution, and an FLT equivalence mod p^k with three terms in core is a (scaled) cubic root solution.*

Lemma 3.2. *The p-th powers of 0-extended terms of a triplet^p (*mod p^k*) yield integer inequality.*

Proof. In a triplet^p for some odd prime p the core increment form (4) holds for three distinct values of $n < p$. Consider each triplet^p equivalence separately. To simplify notation let r be any of the three r_n, and core residues $A_k(n+1) \equiv x^p \equiv x$, $-A_k(n) \equiv y^p \equiv y \mod p^k$. Then $x^p + y^p \equiv x + y \equiv r^p \mod p^k$, where $r^p \equiv 1 \mod p^2$, has both summands in core, but $r^p \not\equiv 1 \mod p^k$ for $k > 2$ is not in core: deviation $d \equiv r - r^p \not\equiv 0 \mod p^k$.

Hence $r \equiv r^p + d \equiv (x + y) + d \mod p^k$ (with $d \equiv 0 \mod p^k$ in the cubic root case), and $x^p + y^p \equiv x + y \equiv (x + y + d)^p \mod p^k$. The corresponding 0-extensions yield integer p-th power inequality: $X^p + Y^p < (X + Y + D)^p$. □

In the case of cubic roots in core A_k, less than full pk digit precision (base p), namely mod p^{3k+1} suffices to yield the FLT inequality (Corollary 2.1). For any triplet^p mod p^2, necessarily in core A_2 (Corollary 1.2), and for cubic roots of 1 mod p^k (any $k > 0$), there holds $(x + y)^p \equiv x + y \equiv x^p + y^p$, where exponent p distributes over a sum. By binomial expansion the sum of mixed terms yields integer $(X + Y)^p - (X^p + Y^p) \neq 0$ of precision kp, which is $0 \mod p^2$ for any triplet^p.

For any triplet^p mod p^k $(k > 2)$, say in core increment form $(5')$, it is conjectured that there is a least precision $m(k)$ (base p), not exceeding that for cubic roots, which implies inequivalence $X^p - Y^p \not\equiv Z^p \mod p^m$ $(Z^p \equiv 1 \mod p^2)$ for successive core 0-extensions $X, Y < p^k$.

Conjecture. *The 0-extensions $X, Y, Z < p^k$ of terms in any triplet^p* mod p^k *equivalence in core increment form* $(5')$ *with $X - Y = Z \equiv 1 \mod p^2$ yield:* $X^p - Y^p \not\equiv Z^p \mod p^{3k+1}$.

4. Relation to Fermat's Small and Last Theorem

Core A_k as FST extension mod p^k $(k > 1)$, the additive zero-sum property of its subgroups (Theorem 1.1), and the triplet structure of units group G_k (Theorem 3.1), allow a direct approach to Fermat's Last Theorem:

(6) $x^p + y^p = z^p$ (prime $p > 2$) has no solution for positive integers $x,\ y,\ z$
with case$_1$: $xyz \not\equiv 0 \mod p$, and case$_2$: p divides one of x, y, z.

Usually (6) mentions exponent $n > 2$, but it suffices to show inequality for primes $p > 2$, because composite exponent $m = p \cdot q$ yields $a^{pq} = (a^p)^q = (a^q)^p$. In case$_2$: p divides just one term, because if p divides two terms then it also divides the third, and all terms can be divided by p^p.

A finite integer FLT solution of (6) has three p-th powers, each less than p^m for some finite fixed $m = kp$, with $x, y, z < p^k$, so (6) holds mod p^m, yet with no carry beyond p^{m-1}, 0-extending all terms.

The present approach needs only a simple form of Hensel's lemma [**5**] (in the general p-adic number theory), which is a direct consequence of Corollary 1.2, extend digit-wise the normed 1-complement form (2′) such that the i-th digit of weight p^i in a^p and b^p sum to $p-1$ $(0 \leq i < k)$, with p choices per extra digit. Thus to each normed solution of (2′) mod p^2 there correspond p^{k-2} solutions mod p^k.

Corollary 4.1 (1-complement extension). *For $k > 2$, a normed FLT_k root is an extended FLT_2 root.*

4.1. Proof of the FLT inequality

Regarding FLT case$_1$, cubic root of 1 and triplet^p are the only (normed) FLT_k roots (Theorem 3.1). Any assumed integer case$_1$ solution has a corresponding equivalent core increment form (4) with two terms in core, which by Lemma 3.2 has no integer extension, contradicting the assumption, as follows :

Theorem 4.1 (FLT case$_1$). *For prime $p > 2$ and integers $x, y, z > 0$ coprime to p equation $x^p + y^p = z^p$ has no solution.*

Proof. An FLT_k $(k > 1)$ solution is a linear transformed extension of an FLT_2 root in core $A_2 = F_2$ (Corollary 4.1). By Lemma 3.2 it has no finite p-th power extension, yielding the theorem. □

In FLT case$_2$ just one of x, y, z is a multiple of p, hence p^p divides one of the three p-th powers in $x^p + y^p = z^p$. Again, any assumed case$_2$ equality can be transformed to an equivalence mod p^p with two terms in core A_p, having no integer extension, contra the assumption.

Theorem 4.2 (FLT case$_2$). *For prime $p > 2$ and positive integers x, y, z, if p divides only one of x, y, z then $x^p + y^p = z^p$ has no solution.*

Proof. In a case$_2$ solution p divides a lefthand term, $x = cp$ or $y = cp$ $(c > 0)$, or the right hand side $z = cp$. Bring the multiple of p to the right hand side, for instance if $y = cp$ then $z^p - x^p = (cp)^p$, while otherwise $x^p + y^p = (cp)^p$. So the sum or difference of two p-th powers coprime to p must be shown not to yield a p-th power $(cp)^p$ for any $c > 0$:

$$x^p \pm y^p = (cp)^p \quad \text{has no solution for integers } x, y, c > 0. \tag{7}$$

Notice that core increment form (4) does not apply here. However, by FST the two lefthand terms, coprime to p, are either complementary or equivalent mod p, depending on their sum or difference being $(cp)^p$. Scaling by s^p for some $s \equiv 1 \bmod p$, so $s^p \equiv 1 \bmod p^2$, transforms one lefthand term into a core residue

$A_p(n)$ mod p^p, with $n \equiv x$ mod p. And translation by adding $t \equiv 0$ mod p^2 yields the other term $A_p(n)$ or $-A_p(n)$ mod p^p, respectively. The right hand side then becomes $s^p(cp)^p + t$, equivalent to t mod p^p. So the assumed equality (7) yields, by two equality preserving tansformations, the next equivalence (8), where $A_p(n) \equiv u \equiv u^p \mod p^p$ (u in core A_p for $0 < n < p$ with $x \equiv n \mod p$) and $s \equiv 1,\ t \equiv 0 \mod p^2$

$$(8)\quad u^p \pm u^p \equiv u \pm u \equiv t \mod p^p\ (u \in A_p),\ \text{with}\ \ u \equiv (sx)^p,$$
$$\pm\, u \equiv \pm(sy)^p + t \mod p^p.$$

Equivalence (8) does not extend to integers, because $U^p + U^p > U + U$, and $U^p - U^p = 0 \neq T$, where U, T are the 0-extensions of u, t mod p^p, respectively. But this contradicts assumed equalities (7), which consequently must be false. □

Note. From a practical point of view the FLT integer inequality with terms less than p^{pk} of a 0-extended FLT_k root (case$_1$) is caused by the *carries* beyond p^k, amounting to a multiple of the modulus p^k, produced in the arithmetic (base p). In the expansion of $(a+b)^p$, the mixed terms *can* vanish mod p^k for some a, b, p. Ignoring the carries yields $(a+b)^p \equiv a^p + b^p$ mod p^k, and the EDS' property is as it were the *syntactical* expression of ignoring the carry (*overflow*) in residue arithmetic. In other words, in terms of p-adic number theory, this means 'breaking the Hensel lift': the residue equivalence of an FLT_k root mod p^k, although it holds for all k >0, *does* imply inequality for integer p-th powers less than p^{pk} due to its special triplet structure, where exponent p distributes over a sum.

Conclusions and Remarks

1. The two symmetries $-n$, n^{-1} determine FLT_k roots, which are necessary for an FLT integer solution. However, these symmetries (automorphisms) do not exist for positive integers.
2. Another proof of FLT case$_1$ might use product $1 \mod p^k$ of FLT_k root terms: $ab \equiv 1$ or $abc \equiv 1$, which is impossible for integers > 1. The p-th power of a k-digit natural requires upto pk digits. Arithmetic mod p^k ignores carries of weight p^k and beyond. Interpreting a given FLT_k equivalence in naturals less than p^k, their p-th powers produce for $p > 2$ carries that cause inequality.
3. Core $A_k \subset G_k$ as extension of FST to mod p^k $k > 1$, and the zero-sum of its subgroups (Theorem 1.1) yielding the cubic FLT root (Lemma 2.1), initiated this work. The triplets were found by analysing a computer listing (Table 2) of the FLT roots mod p^2 for primes $p < 200$.
4. Linear analysis (mod p^2) suffices for root existence (Hensel, Corollary 4.1), but triplet^p core increment form (4) with two successor terms in core requires *quadratic* analysis (mod p^3). Similarly, FLT case$_1$ inequivalence mod p^{3k+1} holds for increments of $C_{k+1} \equiv (C_k)^p$ for 0-extended core A_k.
5. "FLT eqn(1) has no finite solution" and "$[ICS]^3$ has no finite fixed point" are equivalent (Theorem 3.1), yet each $n \in G_k$ is a fixed point of $[ICS]^3$

mod p^k (re: FLT_2 roots imply all roots for $k > 2$, yet no 0-extension to integers).

6. Crucial in finding the arithmetic triplet structure were extensive computer experiments, and the application of *associative function composition*, the essence of semi-groups, to the three elementary functions (Theorem 3.1): successor $S(n) = n+1$, complement $C(n) = -n$ and inverse $I(n) = n^{-1}$, with period 3 for $SCI(n) = -(n+1)^{-1}$ and the other three such compositions. In this sense FLT is not a purely arithmetic problem, but essentially requires non-commutative and associative function composition for its proof.

References

1. Apostol T., *Introduction to Analytical Number Theory,* Springer Verlag, 1976.

2. Benschop N., *The semigroup of multiplication mod p^k, an extension of Fermat's Small Theorem, and its additive structure*, International conference Semigroups and their Applications, Prague, July 1996.

3. Benschop N., *Powersums representing residues mod p^k, from Fermat to Waring*, Computers and Mathematics with Applications, **39**(7–8) (2000), 253–261.

4. Clifford A. and Preston G., *The Algebraic Theory of Semigroups*, AMS survey 7, **1** (1961), 130–135.

5. Hardy G. and Wright E., *An Introduction to the Theory of Numbers*, Oxford University Press 1979.

6. Mohit S and Ram Murty, *Wieferich Primes and Hall's Conjecture*, Comptes Rendus de l'Academie. Science, **20**(1) (1998), 29–32.

7. Patent US-5923888 (July 13, 1999) on a Logarithmic Binary Multiplier, with dual bases 2 and 3 (using 3 as semi-primitive root of 1 mod 2^k).

8. Schwarz S., *The Role of Semigroups in the Elementary Theory of Numbers*, Mathematica Slovaca, **31**(4) (1981), 369–395.

9. Wieferich A., *Zum letzten Fermat'schen Theorem*, J. Reine Angew. Math, **136** (1909), 293–302.

N. F. Benschop, Schoutstraat 4, 5663EZ Geldrop, The Netherlands,
e-mail: `n.benschop@chello.nl` – Amspade Research