

# Extend Fermats Small Theorem to $r^{p-1} \bmod p^3$ for divisors $r$ of $p \pm 1$

NICO F. BENSCHOP *AmSpade Research*, The Netherlands

## Abstract

By  $(p \pm 1)^p \equiv p^2 \pm 1 \pmod{p^3}$  and by the lattice structure of  $Z(\cdot) \bmod q$  for  $q = p \pm 1$  (odd prime  $p$ ) all idempotents taken as naturals  $e < p$  are shown to have distinct  $e^{p-1} \bmod p^3$ , and all divisors  $r$  of  $p - 1$  (resp.  $p + 1$ ) have distinct  $r^{p-1} \bmod p^3$ . Moreover  $2^p \not\equiv 2 \pmod{p^3}$  for prime  $p$ , related to *Wieferich* primes [4] and *FLT* case<sub>1</sub>. It is conjectured that for prime  $p > 2$  some  $g \mid p \pm 1$  is semi primitive root of  $1 \bmod p^k$  ( $k > 2$ ), with units group  $\{-1, g\}^*$ .

**Keywords:** Residue arithmetic, ring  $Z \bmod p^k$ , semigroup, primitive root, units group, Wieferich prime, Fermat, quadratic analysis mod  $p^3$ .

**MSC-class:** 11A07, 11A15, 11D41

## 1 Introduction

In ring  $Z \bmod p^k$  (prime  $p > 2$ ) the group  $G_k$  of units (coprime to  $p$ ) of order  $(p - 1)p^{k-1}$ , is known to be cyclic [1]. For a simplified notation parameter  $p$  (odd prime) is omitted, since the following analysis does not depend on  $p$ . Coprime factors  $p - 1$  and  $p^{k-1}$  yield a units group  $G_k \bmod p^k$  with product structure :

(1)  $G_k \equiv A_k B_k \bmod p^k$  : core  $|A_k| = p - 1$ , extension group  $|B_k| = p^{k-1}$ .

It is readily verified that extension group  $B_k \equiv \{ap + 1\} \bmod p^k$  of order  $p^{k-1}$  has generator  $p + 1$ . And by  $(p - 1)^{p^{m-1}} \equiv p^m - 1 \pmod{p^{m+1}}$ ,  $p - 1$  generates all  $2p^{k-1}$  residues  $\pm 1 \bmod p$  of  $\pm B_k$ . Core  $A_k \equiv \{n^{|B_k|}\} \bmod p^k$  is cyclic of order  $p - 1$  for all  $k > 0$  [6], so  $x^{p-1} \equiv 1 \pmod{p^k}$  for each  $x \in A_k$ , extending Fermat's Small Thm (*FST*) to  $k > 1$ .

Moreover, regarding the known problem of a simple rule for *primitive roots* of  $1 \bmod p^k$  (prime  $p > 2$ ), consider the divisors  $r$  of  $p - 1$ , or of  $p + 1$ . It stands to reason to look for generators of  $G_k$  (primitive roots of  $1 \bmod p^k$ ) among the divisors  $r$  of such powerful generators as  $p - 1$  and  $p + 1$ .

## Boolean lattice of idempotents in $Z(\cdot) \bmod q$

In the lattice of idempotents in  $Z_q(\cdot)$  each pair of complementary idempotents as naturals  $e, f < q$  has sum  $e + f = q + 1$  which, although known, is recalled in the next section. With  $q = p - 1$ , it is shown that the divisors  $r \mid p - 1$  have distinct  $r^{p-1} \in B_3 \bmod p^3$ , and similarly for all  $r \mid p + 1$ . The analysis is via the lattice of idempotents in  $Z(\cdot) \bmod q$  (base  $q = p - 1$ , resp.  $p + 1$ ), which also have this property in  $B_3 \bmod p^3$ .

Notice that no generator  $g$  of  $G_k$  can be in core  $A_k$ , since  $|g^*| = (p - 1)p^{k-1}$ , while the order  $|x^*|$  of  $x \in A_k$  divides  $|A_k| = p - 1$ . So  $p$  (resp.  $p^2$ ) must divide the order of a non-core residue (resp. primitive root of  $1 \bmod p^{k>2}$ ).

**Note.** Residue  $n \bmod p^k$ , with a unique  $k$ -digit representation (base  $p$ ), can be interpreted as non-negative integer  $< p^k$ , its *principle value*, also denoted by  $n$  when no confusion can arise. So  $B_k$  consists of all  $p^{k-1}$   $k$ -digit representations with least significant digit 1, generated as powers of 11 (base  $p$ )  $\bmod p^k$ . Subgroup  $F_k = \{x^p\}$  of  $p$ -th power residues in  $G_k$  has order  $|G_k|/p = (p - 1)p^{k-2}$ , and core  $A_k \bmod p^k$  has order  $p - 1$  for each  $k > 0$ , so  $F_2 = A_2$ .

### Fermat's Small Theorem $\bmod p^k$ extended to $k > 1$

By *FST* :  $x^{p-1} \equiv 1 \bmod p$  (all  $x \not\equiv 0 \bmod p$ ), so all  $0 < x < p$ , also referred to as *natural*  $x < p$ , have equal  $x^{p-1} \bmod p$ .

For odd prime  $p$  the **question** then is:

for which least *precision*  $k$  and natural  $x < p$  do  $x^{p-1} \bmod p^k$  differ, shown to be  $k = 3$  for some naturals  $r < p$ , namely divisors  $r \mid q = p \pm 1$ , and idempotents  $e^2 \equiv e \bmod q$ .

**Def:** the **image** of integer or unit  $x \in G_3$  is residue  $x^{p-1} \bmod p^3$  in  $B_3$ , and  $x = \sum_{i=0}^2 x_i p^i = [x_2, x_1, x_0]$  with digits  $0 \leq x_i < p$  (base  $p$ ) denotes integer  $0 \leq x < p^3$  and also its residue  $\bmod p^3$ .

Regarding the divisors of  $q = p \pm 1$  : if  $p - 1$  (and similarly  $p + 1$ ) has prime structure  $\prod_{i=1}^u p_i^{e_i}$  then there are  $\prod_i (e_i + 1)$  divisors forming a lattice, which is a Boolean lattice in case  $q$  is squarefree.

Divisors  $r \mid p - 1$  with distinct prime divisor sets generate  $2^u$  idempotents  $e^2 \equiv e \bmod q$ , forming a Boolean Lattice [3]. There are as many maximal one-idempotent subsemigroups, the 'Archimedian components' [2] [3] of  $Z_q = Z(\cdot) \bmod q$ . By the lattice structure of semigroup  $Z_q(\cdot)$ , cor3.1:

if  $x \neq y < p$  yet  $x^{p-1} \equiv y^{p-1} \bmod p^3$  then not both  $x, y$  can divide  $p - 1$  (resp.  $p + 1$ ). Two such rare cases for  $p < 4.10^4$  with coprime  $x, y$  are

$$p = 19 : 6^{18} \equiv 11^{18} \equiv [11, 2, 1] \quad \text{and} \quad p = 41 : 7^{40} \equiv 10^{40} \equiv [31, 37, 1].$$

An essential well known result for integers is the following :

**LEMMA 1.1** *Any integer pair  $(r, s)$  is fixed by product  $rs$  and sum  $r + s$ .*

**PROOF.** Let  $r + s = b$  and  $rs = c$ . Substitute  $s = c/r$  then  $r^2 - br + c = 0$  with

two roots  $(r, s) = (b \pm \sqrt{b^2 - 4c})/2$ . Determinant  $b^2 - 4c = (r + s)^2 - 4rs = (r - s)^2$  is indeed a perfect square, with integers  $r, s$ .  $\square$

## 1.1 Divisors $r \mid p \pm 1$ and residues $(p \pm 1)^p \bmod p^3$

Recall  $FST : x^{p-1} \equiv 1 \pmod p$  (prime  $p > 2$ , natural  $x < p$ ) and the question for which  $k$  all are distinct mod  $p^k$ . Rare case  $p=113$  has  $68^{112} \equiv 1 \pmod{p^3}$ , showing  $k > 3$  if all  $x^{p-1} \pmod{p^k}$  are to be distinct.

Notice both addition and multiplication are associative and commutative, while exponentiation is neither. Positive integer arithmetic misses the two symmetries (automorphisms of order 2) of residue arithmetic mod  $p^k$ :

additive complement  $-x$ , and multiplicative inverse  $x^{-1}$  of units.

Note:  $(x_1p + x_o)^p \equiv x_o^p \equiv c_o p + x_o \pmod{p^2}$  has carry  $c_o$  independent of  $x_1$ . The known binomial expansion (Pascal's triangle) relates addition to exponentiation. In quadratic analysis (mod  $p^3$ ) the  $p$ -th power of  $p \pm x$  yields  $\pm x^p$  translated over  $p^2$ , due to  $FST$ :

$$(2a) \quad (p \pm x)^p \equiv x^{p-1}p^2 \pm x^p \equiv p^2 \pm x^p \pmod{p^3}, \text{ for } x \not\equiv 0 \pmod p.$$

A 'shift' (base  $p$ ) over  $m$  positions results by taking  $m$  times the  $p$ -th power:

$$(2b) \quad (p \pm 1)^{p^m} \equiv p^{m+1} \pm 1 \pmod{p^{m+2}} \implies r^p \not\equiv r \pmod{p^3} \text{ for } r = p \pm 1.$$

This shift in  $p$ -th power residues (base  $p$ ) causes distinct  $r^{p-1} \pmod{p^3}$  for all divisors  $r \mid p \pm 1$  (cor.3.1), so  $r^{p-1} \equiv 1 \pmod{p^3}$  only if  $r=1$ . In fact :  $rs = p - 1 \implies r^p s^p \equiv p^2 - 1 \not\equiv rs \pmod{p^3}$  so:  $r^p \not\equiv r$  and/or  $s^p \not\equiv s \pmod{p^3}$ . It will be shown that 'and' holds here, for any pair of cofactors  $r, s$ .

**Note:** Additive  $p$ -th power anti-closure property  $x^p + y^p \neq z^p$  for all integers  $x, y, z$  coprime to  $p$  ( $FLT$  case<sub>1</sub>) holds if  $2^p \not\equiv 2 \pmod{p^2}$ , true for all primes  $p < 4.10^{12}$  except 'Wieferich primes' 1093, 3511: with  $2^p \equiv 2 \pmod{p^2}$  [4] [5]. And  $2 \mid p \pm 1$  for all odd primes suggests to study more generally  $r \mid p \pm 1$ .

Many primes have  $x^p \equiv x \pmod{p^2}$  for some  $1 < x < p$ . Table 1 lists the 60 cases in 43 of the 78 odd primes  $p \leq 401$ , with one case of  $r \mid p + 1 : 3 \mid 11 + 1$ , and four cases of  $r \mid p - 1$  denoted  $r(p) : 14(29), 18(37), 20(281), 104(313)$ . Note:  $68^{113-1} \equiv 1 \pmod{p^3}$  with 68 not dividing  $113 \pm 1$ .

## 2 Lattice structure of semigroup $Z(.) \bmod q$

The divisors of  $q = p \pm 1$  are best studied in  $Z(.) \bmod q$ , followed by base transfer  $q \rightarrow p$ , for their properties mod  $p^3$ . Recall the lattice structure [2] [3] of multiplicative semigroup  $Z_q(.)$  of residues mod  $q$ , to be applied for  $q = p - 1$ , and  $q = p + 1$  respectively.

**Def:** For natural  $q$  : 'primeset'  $P(q)$  is the set its prime divisors.

**Def:**  $P(x)$  ,  $0 < x \leq q$  is the set of prime divisors common to  $x$  and  $q$ .

Hence  $P(x) \subseteq P(q)$ , and for the units  $u < q$  of  $Z_q$  :  $P(u) = \emptyset$ . Moreover  $P(xy) = P(x) \cup P(y)$  and  $P(x^n) = P(x)$  for  $n > 0$ . Denote  $P(q) = P(0)$ , since  $q \equiv 0 \pmod q$ . Let  $x^*$  be the 'iteration class' of all distinct powers  $x^n \in Z_q$ , which is known to contain precisely one idempotent  $x' \equiv (x')^2$ .

Let modulus  $q$  be the product of  $u$  coprime factors  $p_i^{e_i}$ .

Then  $Z_q$  is the direct product of  $u$  semigroups  $Z(\cdot) \pmod{p_i^{e_i}}$ .

**Def:** An Archimedian component of  $Z_q$  , or briefly 'P-component', consists of all residues  $x$  generating idempotent  $e$  , with primeset  $P(x) = P(e)$  [2].

These are the  $2^u$  maximal one-idempotent subsemigroups of  $Z_q$  , one per idempotent resp. subset of  $P(0) = P(q)$ . Their (partial) ordering is that of commuting idempotents  $e^2 \equiv e$ ,  $f^2 \equiv f$ ,  $ef \equiv fe$ .

**Def:** idempotent ordering  $e \supseteq f$  denotes  $ef \equiv fe \equiv f$  in  $Z_q(\cdot)$  :

$$e \text{ is identity for } f \iff P(e) \subseteq P(f) ,$$

$$\text{with lattice top } 1 : P(1) = \emptyset, \text{ and bottom } 0 : P(0) = P(q).$$

Notice this ordering differs from the arithmetic ordering  $e \geq f$  of idempotents as naturals  $< q$  , to be used later as well.

Semigroup  $Z_q(\cdot)$  is the disjoint union of its Boolean lattice of P-components. It is readily verified that if  $1 \in x^*$  then iteration class  $x^*$  is a cycle (cyclic group). In fact all  $x$  that generate 1, the semigroup identity, form a group  $G(1)$  ordered at the lattice top. Such  $x$  must be coprime to  $q$ , hence is a 'unit' of  $Z_q$ , so primeset  $P(1) = \emptyset$  is empty, and  $P(0) = P(q) = \{p_i\}$  is the full primeset of  $q$ , with trivial subgroup  $G(0) \equiv 0$  as lattice bottom idempotent.

**Def:** Denote by  $r'$  the idempotent generated by  $r$  in  $Z_q$  .

The product  $eg \pmod q$  of two idempotents is idempotent since :

$$(eg)^2 \equiv egeg \equiv eegg \equiv eg ,$$

so Boolean lattice  $L_q(\cdot)$  of idempotents is closed under multiplication.

Recall each pair of idempotents  $a \neq b$  to yield a pair  $(e, g)$  of idempotents with:  $(a + b)' = e \neq g = ab \in L_q$  having primesets  $P(e) = P(a) \cup P(b)$  and  $P(g) = P(a) \cap P(b)$  and ordering  $e \supseteq \{a, b\} \supseteq g$  in  $L_q$  , respectively least upper bound  $e = lub(a, b)$  and greatest lower bound  $g = glb(a, b)$ .

If  $a, b$  are not ordered, then each such quadruple  $e \supset \{a, b\} \supset g = ab$  forms a sublattice which is a direct product of two ordered pairs in  $L_q$  and its four idempotents have distinct images mod  $p^3$  (thm 2.2).

## 2.1 Distinct $e^{p-1} \pmod{p^3}$ for idempotents $e \in Z_{p-1}$

Divisors  $r \mid q = p - 1$  with differing primesets are in distinct P-components of  $Z_q(\cdot)$  with different idempotents  $r' \pmod q$ , shown to yield distinct  $(r')^{p-1}$

mod  $p^3$  (*combinational* inequivalence). The powers  $r^n \bmod q$  of  $r$  are in one  $P$ -component. If  $r^{p-1} \equiv cp + 1 \bmod p^3$  has carry  $c \not\equiv 0 \bmod p^2$  then power residues  $(r^n)^{p-1} \equiv mcp + 1 \bmod p^3$  where  $m$  depends on  $n$ , with resulting *sequential* inequivalence mod  $p^3$ , considered next.

LEMMA 2.1 :

Each pair of complementary idempotents  $e, f \in Z_q$  (**co-idempotents**) as naturals  $e, f < q$  satisfies, for any base  $q > 1$  :

$$P(e) \cup P(f) = P(q) = P(0) \quad \text{and} \quad P(e) \cap P(f) = P(1) = \phi, \quad \text{with} :$$

$$(3a): \quad ef \equiv 0 \pmod{q}, \quad \text{and} \quad (3b): \quad e + f \equiv 1 \pmod{q}.$$

PROOF. (3a) is obvious, and (3b) is verified as follows. Notice (3a) implies  $e + f$  is idempotent, since  $(e + f)^2 \equiv e^2 + f^2 + 2ef \equiv e + f \pmod{q}$ .

Moreover  $ef \equiv 0$  implies :  $e + f$  is identity for  $e$  because  $(e + f)e \equiv e(e + f) \equiv e^2 + ef \equiv e \implies e + f \supseteq e$ . Similarly  $e + f \supseteq f$ . Hence  $e + f$  is identity for both idempotents  $e, f \in Z_q$  and  $e + f$  is coprime to  $q$ , so it must be the lattice identity  $1 \bmod q$ .  $\square$

Taking  $q = p - 1$  then  $e + f = p$  so  $e, f$  are complementary mod  $p$ .

Using (3) any pair of co-idempotents  $e, f$  **as naturals**  $< p$  satisfies :

$$(4a) \quad ef = m_{ef}(p - 1) \quad \text{where} \quad 1 \leq m_{ef} < p, \quad \text{and:}$$

$$(4b) \quad e + f = p. \quad \text{By (2a) : } e^p = (p - f)^p \equiv p^2 - f^p \pmod{p^3}, \quad \text{so :}$$

$$(4c) \quad e^p + f^p \equiv p^2 \pmod{p^3}.$$

LEMMA 2.2 *Distinct co-idempotent pairs in  $Z_{p-1}$  as naturals  $e, f < p$  have distinct products  $ef = m_{ef}(p - 1)$ , hence different  $m_{ef} < p$ .*

PROOF. By (4b) all co-idempotent pairs have sum  $p$ , so by lem1.1 and (4a) they have distinct products:  $ef = m_{ef}(p - 1)$ , thus distinct  $m_{ef} < p$ .  $\square$

LEMMA 2.3 *For co-idempotent pairs  $e, f \in Z_{p-1}$  :  $e^{p-1} \not\equiv f^{p-1} \pmod{p^3}$ .*

PROOF. By (4b):  $e^{p-1} \equiv (p - f)^p / (p - f) \equiv (p^2 - f^p) / (p - f) \not\equiv f^{p-1} \pmod{p^3}$  since  $f^{p-1}(p - f) \not\equiv p^2 - f^p \pmod{p^3}$ , where  $f^{p-1} \not\equiv p \pmod{p^2}$  (by *FST*).  $\square$

Notice minimal value  $m_{ef} = 1$  for  $(e, f) = (1, p - 1)$ . By (4b,c) and *FST* at most one of  $e^p \equiv e, f^p \equiv f \pmod{p^3}$  can hold. In fact only  $e = 1$  yields equivalence, with  $f = p - 1$  so  $f^p \equiv (p - 1)^p \equiv p^2 - 1 \not\equiv f \pmod{p^3}$ , and inequivalence  $x^p \not\equiv x \pmod{p^3}$  holds for all idempotents  $x \neq 1$ , shown next.

Idempotent  $e^2 \equiv e \pmod{q}$  ( $q = p - 1$ ) implies  $e^2 = c(p - 1) + e < q^2$  for some carry  $0 \leq c < q$ . Notice :

$$(5) \quad c = 0 \iff e = 1, \text{ and } e > 1 \implies e^2 > q \implies e > \sqrt{p-1}.$$

LEMMA 2.4 For co-idempotents  $e, f \in Z_q$  :  $e^2 = cq + e$ ,  $f^2 = dq + f$  :

(6a) the carries  $0 \leq c, d < q = p - 1$  satisfy:  $c < e$ ,  $d < f$ .

(6b) By (4a):  $ef = m(p - 1)$  where:  $m = e - c = f - d < q$ .

PROOF. (6a):  $p > e \implies ep > e^2$ , hence :

$$e(p - 1) + e > c(p - 1) + e \implies e > c, \text{ and similarly } f > d.$$

$$(6b): \quad e^2 - f^2 = (e - f)(e + f) = (e - f) + (c - d)q,$$

$$\text{and by (4b): } (e - f)p - (e - f) = (e - f)q = (c - d)q.$$

So :  $e - f = c - d$  and  $e - c = f - d$  ..(\*) Moreover by  $e + f = p = q + 1$  :

$$(e + f)^2 = (q + 1)^2 \implies e^2 + f^2 + 2ef = (c + d)q + q + 1 + 2mq = q^2 + 2q + 1$$

Hence  $(c + d)q + 2mq = q^2 + q \implies c + d + 2m = q + 1 = e + f$ , yielding :

$$(e - c) + (f - d) = 2m, \text{ and with (*) follows: } e - c = f - d = m < q. \quad \square$$

THEOREM 2.1 : (odd prime  $p$ )

For idempotents  $e \in Z_{p-1}$  as naturals  $e < p$  :  $e^p \equiv e \pmod{p^3} \implies e = 1$ .

PROOF. By (4a,b):  $ef = e(p - e) = m(p - 1)$  where  $m = m_{ef} < p$ ,

so  $e = m \iff e = 1$ . Take  $p$ -th powers, and use  $p^2 - 1 = (p - 1)(p + 1)$  :

$$e^p(p^2 - e^p) \equiv m^p(p^2 - 1) \equiv e(p - e)(p + 1)m^{p-1} \pmod{p^3}.$$

By FST :  $m^{p-1} = xp + 1$  for some  $x \geq 0$ . Then  $e^p \equiv e \pmod{p^3}$  yields :

$$p^2 - e \equiv (p - e)(p + 1)(xp + 1) \equiv (p - e)(p + 1)xp + p - ep + (p^2 - e) \pmod{p^3}.$$

So  $(p - e)(p + 1)x \equiv e - 1 \pmod{p^2}$ . Discard  $p^2$  then:

$$(7) \quad -(e - 1)xp - xe \equiv e - 1 \pmod{p^2}.$$

Use  $1 \leq e < p$ , so that for residues mod  $p$  holds :

$$-xe \equiv e - 1 \pmod{p} \implies 1 \equiv (x + 1)e \implies x \equiv e^{-1} - 1 \pmod{p}.$$

Then by (7):

$$-(e - 1)(e^{-1} - 1)p - (e^{-1} - 1)e \equiv -[2 - (e + e^{-1})]p - (1 - e) \equiv e - 1 \pmod{p^2}$$

so:  $2 \equiv e + e^{-1} \iff 2e \equiv e^2 + 1 \iff (e - 1)^2 \equiv 0 \pmod{p} \implies e = 1$  by (5).

□

THEOREM 2.2 :

All idempotents  $e \in Z_{p-1}$ , as naturals  $e < p$ , have distinct  $e^{p-1} \pmod{p^3}$ .

PROOF. For ordered idempotents  $e \supset a$  holds  $e^q \not\equiv a^q \pmod{p^3}$ . Because  $a \equiv ge \pmod{q}$  for some idempotent  $g \subset 1$  with  $g^q \not\equiv 1 \pmod{p^3}$  (thm2.1), so  $a^q \equiv g^q e^q \not\equiv e^q \pmod{p^3}$  in  $B_3$ .

Non-ordered idempotents  $a \not\equiv b$  have  $a \subset 1, b \subset 1$  so  $a^q \not\equiv 1, b^q \not\equiv 1 \pmod{p^3}$  (thm2.1) and let  $glb(a, b) \equiv z \equiv ab$ . Assume  $a^q \equiv b^q \pmod{p^3}$  then  $z^q \equiv a^q b^q \equiv (a^2)^q \pmod{p^3}$ . But ordered pair  $z \subset a \equiv a^2 \pmod{q}$  yields different images, falsifying the assumption, so  $a^q \not\equiv b^q \pmod{p^3}$ .  $\square$

### 3 Distinct $r^{p-1} \pmod{p^3}$ for divisors $r \mid p \pm 1$

Let  $r_n < p$  be the natural representing residue  $r^n \pmod{q}$ , with  $q = p - 1$ .

**Def:** Divisors of  $p - 1$  with the same set of prime divisors are defined as *equivalent divisors*.

Notice they generate the same idempotent in  $Z_{p-1}$ .

The fact that the idempotents of  $Z_{p-1}$  have distinct images  $e^{p-1} \pmod{p^3}$  (thm.2.1) implies the same property for non-equivalent divisors of  $p - 1$ , seen as follows.

**THEOREM 3.1** For odd prime  $p$  :

*Non-equivalent divisors  $r \mid p - 1$  have distinct images  $r^{p-1} \pmod{p^3}$ .*

PROOF. Each divisor  $r$  of  $q = p - 1$  generates in semigroup  $Z_{p-1}(\cdot)$  a unique idempotent  $r' \pmod{q}$ . By theorem 2.2 these idempotents generate as many distinct images  $(r')^{p-1} \pmod{p^3}$ .

Assume non-equivalent divisors  $(r, s)$  to generate the same image  $r^{p-1} \equiv s^{p-1} \equiv t \pmod{p^3}$ . Let  $r' \equiv r^m$  and  $s' \equiv s^n$  with  $k = lcm(m, n)$  then  $r' \equiv r^k$  and also  $s' \equiv s^k$ . But  $r^{p-1} \equiv s^{p-1} \implies r^{(p-1)k} \equiv s^{(p-1)k} \implies (r')^{p-1} \equiv (s')^{p-1}$ . So the assumption of equal image implies the same idempotent image, contradicting theorem 2.1.

Hence non-equivalent divisors (distinct idempotents) have distinct images.  $\square$

Notice  $2 \mid p - 1$  for all odd primes  $p$ , and  $2^p \not\equiv 2 \pmod{p^3}$  for  $p=2$ , so by thm.2.1 ( $e^p \equiv e$  only for  $e=1$ ):

**COROLLARY 3.1** For prime  $p$  :  $2^p \not\equiv 2 \pmod{p^3}$ .

Notice 2 divides  $p - 1$  for all odd primes  $p$ , and by inspection for  $p = 2$  :

**COROLLARY 3.2** For prime  $p$  :  $2^p \not\equiv 2 \pmod{p^3}$ .

### 3.1 Idempotents of $Z_{p+1}(\cdot)$ and divisors of $p + 1$

Similar to (4a,b) for modulus  $p - 1$ , consider  $q = p + 1$  (prime  $p > 2$ ). Then for  $u$  prime divisors of  $p + 1$  the  $2^{u-1}$  co-idempotent pairs  $e, f \in Z_{p+1}$  satisfy, with as many distinct multiples  $m_{ef}$ :

$$(8a) \quad ef = m_{ef}(p + 1) \quad \text{where } 1 \leq m_{ef} \leq p + 1$$

$$(8b) \quad e + f = p + 2.$$

As naturals the trivial pair  $(1, p + 1)$  has images 1 and  $(p + 1)^{p-1} \equiv (p^2 + 1)/(p + 1) \equiv 2p^2 - p + 1 \equiv p^2 + (p - 1)p + 1 \pmod{p^3}$ . And by theorem 2.1, only trivial idempotent 1 has image 1 mod  $p^3$ , hence similarly follow:

**THEOREM 3.2** (odd prime  $p$ ):

The idempotents  $e \in Z_{p+1}$  as naturals  $e \leq p + 1$  have distinct  $e^{p-1} \pmod{p^3}$

**COROLLARY 3.3** (odd prime  $p$ ):

All divisors  $r \mid p + 1$  have distinct images  $r^{p-1} \pmod{p^3}$ .

#### Notes:

1. Units group  $G_k \equiv g^* \pmod{p^{k>2}}$ : prime  $p$  divides its order  $|g^*| = (p - 1)p^{k-1}$ . So  $g$  is not in core  $A_3$  of order  $p - 1$ , which by thm3.1 is satisfied if  $g \mid (p \pm 1)$ , but this is not sufficient. Moreover,  $p=73$  ( $G_k = 5^*$ ) is the smallest prime with no primitive root  $r \mid p \pm 1$ , although 6, 12 and their cofactors do generate half of  $G_k$ , in fact missing  $-1 \pmod{p^k}$ . The next such case is  $p = 193$  with no  $r \mid p \pm 1$  units generator, yet with semigenerators 2, 6, 32, 96, 97.

For most primes it appears that at least one of  $(p \pm 1)/2$  is a semigenerator.

**Conjecture:** Some divisor  $r \mid p \pm 1$  is a *semi* primitive root of 1 mod  $p^k$  for  $k > 2$ , with  $G_k = \{-1, r\}^*$  and  $|r^*| = p^{k-1}(p - 1)/2$ .

2. It is known [1] that  $G_k$  is cyclic (one generator) for odd primes  $p$  and any precision  $k \geq 1$ , but not for  $p=2$  and  $k \geq 3$  (re: the multiplicative Klein group  $G_3 = C2 \times C2$  of odd residues mod  $2^3$ , a direct product of 2-cycles), due to  $(p + 1)^2 > p^3$  only for  $p=2$ . With trivial core of order  $p - 1 = 1$ , the units mod  $2^{k>2}$  have semi-generator  $p+1=3$  with  $\{3, -1\}$  generating all  $2^{k-1}$  units [7].

3. Recall an old result of Wieferich (1909) [4][5]: "If  $2^p \not\equiv 2 \pmod{p^2}$  for odd prime  $p$  then *FLT* case<sub>1</sub> holds for exponent  $p$ ." (that is:  $x^p + y^p \neq z^p$  for all natural  $x, y, z$  coprime to  $p$ ). The Wieferich inequivalence holds at least for all primes  $p < 4.10^{12}$ , except 1093 and 3511. If his could be extended to  $2^p \pmod{p^3}$ , then *FST'* mod  $p^3$  (cor3.2) would yield a direct proof of *FLT* case<sub>1</sub>.

4. The finite precision nature is characterized by a *critical precision* of 3, corresponding to quadratic analysis mod  $p^3$ . This concept was applied in [6]

to study the range of residues covered by the pair sums of  $p$ -th power units  $a^p + b^p \pmod{p^k}$ , shown to cover half the units group  $G_k$  for  $k \geq K_p$ , thus of at least critical precision  $K_p$  for prime  $p$ , which for most primes is  $K_p = 2$ . The results presented here extend a side result (thm3.1) in [6].

3( 11)+	-2( 11)	14( 29)-	18( 37)-	19( 43)
-6( 59)	11( 71)	26( 71)	31( 79)	-44( 97)
43(103)	-13(109)	-45(113)<	38(127)	62(127)
58(131)	-20(131)	19(137)	-73(151)	65(163)
-79(163)	78(181)	-15(191)	-54(197)	-25(199)
-46(211)	-29(211)	69(223)	44(229)	-20(229)
33(233)	94(241)	48(257)	79(263)	-98(269)
-89(269)	-62(269)	20(281)-	-136(283)	91(293)
40(307)	104(313)-	-100(313)	18(331)	71(331)
-7(331)	75(347)	156(347)	-126(349)	-32(349)
14(353)	-157(353)	-102(359)	-28(359)	159(367)
-162(367)	-131(373)	174(379)	175(397)	-121(401)

$n(p)+ : n|p+1, \quad n(p)- : n|p-1. \quad p=113: 68^{[p-1]}=001$

Table 1: All cases  $1 < n < p-1$  with  $n^p = n \pmod{p^2}$  (prime  $p < 402$ )

## References

1. T. Apostol: "*Introduction to Analytic Number Theory*" (thm 10.4-6), Springer Verlag, 1976.
2. A. Clifford, G. Preston: *The Algebraic Theory of Semigroups* Vol 1 (p130 -135), AMS survey #7, 1961.
3. S. Schwarz: "The Role of Semigroups in the Elementary Theory of Numbers", *Math.Slovaca* V31, N4, p369-395, 1981.
4. A. Wieferich: "Zum letzten Fermat'schen Theorem", *J. Reine Angew. Math*, V136 (1909) 293-302.
5. S. Mohit, M. Ram Murty: "Wieferich Primes and Hall's Conjecture", *Comptes Rendus de l'Acad. Science (Canada)*, V20, N1 (1998) 29-32.
6. N. Benschop: "Powersums representing residues mod  $p^k$ , from Fermat to Waring", *Comp. and Math. with Appl's*, V39 N7-8 (2000) 253-261.
7. Patent US-5923888 (13 July 1999) on a Logarithmic Binary Multiplier (dual bases 2 and 3).