Exponent of local ring extensions of Galois rings and digraphs of the kth power mapping

Yotsanan Meemark

Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University, Bangkok, Thailand

http://pioneer.netserv.chula.ac.th/~myotsana/

4 July 2016

Overview

Digraph of the kth power mapping

Let R be a finite commutative ring with identity $1 \neq 0$. For an integer $k \geq 2$, the **kth power mapping digraph over R**, denoted by $G^{(k)}(R)$, is the digraph whose vertex set is R and there is a directed edge from a to b if and only if $a^k = b$.

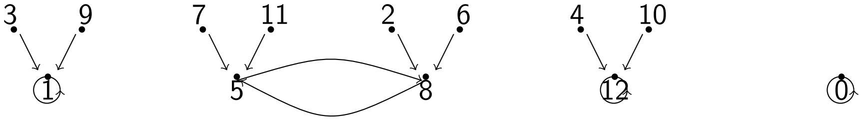
We consider two disjoint subdigraphs:

$G_1^{(k)}(R)$ induced on the set of vertices in the unit group $R^\times$ and

$G_2^{(k)}(R)$ induced on the remaining vertices which are not invertible.

Example

The digraph $G^{(3)}(\mathbb{Z}_{13})$.



Timeline

Křížek and Somer studied the digraphs $G^{(2)}(\mathbb{Z}_n)$ and $G^{(k)}(\mathbb{Z}_n)$.

2004

Křížek M., Somer L.: On a connection of number theory with graph theory, *Czechoslovak Math. J.* **54** (2004), 465–485.

2009

Křížek M., Somer L.: On symmetric digraphs of the congruences $x^k \equiv y \pmod{n}$, *Discrete Math.* **309** (2009), 1999–2009.

Křížek and Somer's tool

The Carmichael λ-function which is defined by a modification of the Euler's φ-function as follows:

1. $\lambda(1) = 1 = \varphi(1)$, $\lambda(2) = 1 = \varphi(2)$, $\lambda(4) = 2 = \varphi(4)$.
2. $\lambda(2^k) = 2^{k-2} = \frac{1}{2}\varphi(2^k)$, for $k \geq 3$.
3. $\lambda(p^k) = (p-1)p^{k-1} = \varphi(p^k)$, for any odd prime p and $k \geq 1$.
4. $\lambda(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}) = \mathrm{lcm}(\lambda(p_1^{k_1}), \lambda(p_2^{k_2}), \dots, \lambda(p_r^{k_r}))$, where $p_1, p_2, \dots, p_r$ are distinct primes and $k_i \geq 1$ for $i \in \{1, \dots, r\}$.

Timeline

Meemark and Wiroonsri worked on the digraphs $G^{(2)}(\mathbb{F}_{p^n}[x]/(f(x)))$ and $G^{(k)}(\mathbb{F}_{p^n}[x]/(f(x)))$ where $f(x)$ is a monic polynomial of degree ≥ 1 in $\mathbb{F}_{p^n}[x]$.

2010

Meemark Y., Wiroonsri N.: The quadratic digraph on polynomial rings over finite fields, *Finite Fields Appl.* **16** (2010), 334–346.

2012

Meemark Y., Wiroonsri N.: The digraphs of the kth power mapping of the quotient ring of polynomial ring over finite fields, *Finite Fields Appl.* **18** (2012), 179–191.

Timeline

Meemark found that we can replace Carmichael λ-function with the "exponent" of the unit group of $\mathbb{F}_{p^n}[x]/(f(x))$.

2011

Meemark Y., Maingam N.: The digraphs of the square mapping on quotient rings over the Gaussian integers, *Int. J. Number Theory*. **7** (2011), 835–852.

2012

Su H.D., Tang G.H., Wei Y.J.: The square mapping graphs of finite commutative rings, *Algeb. Collo.* **19** (3) (2012), 569–580.

Timeline

2014

Nan J.H., Tang G.H., Wei Y.J.: The iteration digraphs of group rings over finite fields, *Algebra and Its Appl.* **5** (2014), 1–19.

2015

Tang G.H., Wei Y.J.: The iteration digraphs of finite commutative rings, *Turk. J. Math.* **39** (2015), 872–883.

2015

Deng G., Somer L.: On the symmetric digraphs from the kth power mapping on a finite commutative ring, *Discrete Math., Algorithms and Appl.*, Vol.7, No.1 (2015), 1–15.

Exponent of a finite group

Let G be a finite group. The **exponent of** G, denoted by $\exp G$, is the least positive integer n such that $g^n = e$ for all $g \in G$.

1. $\exp G$ divides $|G|$
2. $\exp G = \mathrm{lcm}\{o(a) : a \in G\}$
3. If $G = G_1 \times G_2$, then $\exp G = \mathrm{lcm}(\exp G_1, \exp G_2)$.

E.g., $\exp \mathbb{Z}_n = n$ and $\exp S_4 = 12$.

Exponent of a finite ring

For a finite ring R with identity, we write $R^\times$ for the group of units of R. The **exponent of** R, denoted by $\lambda(R)$, is defined to be the exponent of the group of units of R. That is, $\lambda(R) = \exp(R^\times)$.

1. We can easily determine the exponent of R if the structure of the group of units is known, such as when R is the ring of integers modulo m, finite fields, Galois rings, and finite chain rings.
2. The exponent of the ring of integers modulo m is the "Carmichael λ-function".

Local rings whose unit group structure is known

A **local ring** R is a commutative ring with unique maximal ideal M. We call the field $k = R/M$ the **residue field**. E.g., every field is a local ring and $\mathbb{Z}_{p^n}$ is a local ring.

- Finite fields: $\mathbb{F}_q$
- $\mathbb{Z}_{p^s}$ where p is a prime and $s \in \mathbb{N}$
- Galois rings: $\mathbb{Z}_{p^n}[t]/(g(t))$ where $g(t)$ is irreducible in $\mathbb{Z}_p[t]$
- Finite chain rings: finite commutatitive local rings with unique *principal* maximal ideal (Hou X.D., Leung K.H., Ma S.L.: On the group of units of finite commutative chain rings, *Finite Fields Appl.* **9** (2003), 20–38.)

Galois rings

Let n, d be positive integers and p a prime.

1. We know that there exists a monic polynomial $g(t)$ in $\mathbb{Z}_{p^n}[t]$ of degree d such that the reduction $\overline{g}(t)$ in $\mathbb{Z}_p[t]$ is irreducible.
2. Consider the ring extension $\mathbb{Z}_{p^n}[t]/(g(t))$ of $\mathbb{Z}_{p^n}$. It is called a **Galois extension** of $\mathbb{Z}_{p^n}$.
3. Up to isomorphism the Galois extension with parameters n, d and p is unique. Hence, we may denote $\mathbb{Z}_{p^n}[t]/(g(t))$ by $GR(p^n, d)$, and call it the **Galois ring**.
4. Observe that $GR(p^n, 1) = \mathbb{Z}_{p^n}$ and $GR(p, d) = \mathbb{F}_{p^d}$.

Galois rings

Theorem

1. *$GR(p^n, d)$ is a finite local ring of characteristic p^n and of order p^{nd} with maximal ideal $M = p(GR(p^n, d))$, which is principal, and residue field $R/M \cong \mathbb{F}_{p^d}$.*
2. *The unit group $GR(p^n, d)^\times \cong H \times \mathbb{F}_{p^d}^\times$, where H is a group of order $p^{(n-1)d}$ such that:*
   a. *If (p is odd) or ($p = 2$ and $n \leq 2$), then H is a direct product of d cyclic groups each of order p^{n-1}, and so the exponent of $GR(p^n, d)$ in this case is $p^{n-1}(p^d - 1)$.*
   b. *If $p = 2$ and $n \geq 3$, then H is a direct product of a cyclic group of order 2, a cyclic group of order 2^{n-2} and $d - 1$ cyclic groups each of order 2^{n-1}, and so the exponent of $GR(2^n, d)$ in this case is $2^{n-1}(2^d - 1)$ for $d \geq 2$ and 2^{n-2} for $d = 1$, respectively.*

Local extensions

An extension ring S of a local ring R is called a **local extension** if S is a local ring. Hence, the Galois ring $GR(p^n, d)$ is a local extension of $\mathbb{Z}_{p^n}$. The next result is well known.

Theorem

Let R be a finite local ring, and $f(x)$ be a monic irreducible polynomial in $R[x]$. Then $R[x]/(f(x)^a)$ is a finite local ring for any $a \in \mathbb{N}$.

Main results

Consider a local extension of the Galois ring $GR(p^n, d)$ of the form

$$R = GR(p^n, d)[x]/(f(x)^a),$$

where $a \geq 1$ and $f(x)$ is a monic polynomial in $GR(p^n, d)[x]$ of degree r such that the reduction $\overline{f}(x)$ in $\mathbb{F}_{p^d}[x]$ is irreducible.

R is a local ring of characteristic p^n with maximal ideal

$$\begin{aligned} M &= (p, f(x))/(f(x)^a) \\ &= \{h(x) + f(x)l(x) + (f(x)^a) : h(x) \in pGR(p^n, d)[x], \\ &\qquad l(x) \in GR(p^n, d)[x], \deg h < r, \deg l < r(a-1)\}. \end{aligned}$$

We shall proceed to compute the "exponent of R" without completely determination of its unit group structure

$a = 1$

When $a = 1$, it turns out that R is still a Galois ring as a result of the next theorem.

Theorem

Let $f(x) \in GR(p^n, d)[x]$ be a monic polynomial of degree r such that the reduction $\overline{f}(x)$ in $\mathbb{F}_{p^d}[x]$ is irreducible. Then the ring $GR(p^n, d)[x]/(f(x))$ is isomorphic to a Galois ring $GR(p^n, dr)$.

Hence, $R = GR(p^n, d)[x]/(f(x)) \cong GR(p^n, dr)$ and the exponent of R is presented in previous theorem.

$a \geq 2$

Deng and Somer (2015) considered the exponent of the ring $\mathbb{F}_{p^n}[x]/(f(x)^a)$, where $a \geq 2$ and $f(x)$ is an irreducible polynomial in $\mathbb{F}_{p^n}[x]$ of degree r in the following theorem.

Theorem

Let $f(x)$ be an irreducible polynomial in $\mathbb{F}_{p^n}[x]$ of degree r and $a \geq 2$. Then

$$\lambda(\mathbb{F}_{p^n}[x]/(f(x)^a)) = p^s(p^{nr} - 1),$$

where $p^{s-1} < a \leq p^s$ for some $s \in \mathbb{N} \cup \{0\}$.

1. Since R is a local ring with maximal ideal M, we have $R^\times \cong (1+M) \times \mathbb{F}_{p^{dr}}^\times$ and $\mathbb{F}_{p^{dr}}^\times$ is cyclic of order $p^{dr}-1$, so it suffices to determine the exponent of the p-group $1+M$.

2. Following Deng and Somer, let s be the positive integer such that $p^{s-1} < a \leq p^s$. We shall show that every element in $1+M$ is of order not exceeding p^{s+n-1} and the order of $1+f(x)+(f(x)^a)$ is p^{s+n-1}, so the exponent of the group $1+M$ is p^{s+n-1}.

3. However, our computation is more complicated because the characteristic of the ring R is p^n and the binomial coefficients do not disappear easily like in the extension of fields case where it is of characteristic p.

For $m \in \mathbb{N}$, we write $e_p(m)$ for **the maximum power of p in m**, that is, $p^{e_p(m)} \mid m$ but $p^{e_p(m)+1} \nmid m$.

The proof is started by deriving some facts on the maximum power of p is binomial coefficients using de Polignac formula.

Theorem (de Polignac formula)

Let $m \in \mathbb{N}$ and p be a prime. Then

$$e_p(m!) = \sum_{i=1}^{\infty} [\frac{m}{p^i}].$$

We divide the computation into four lemmas as follows.

Lemma 1

Lemma

$e_p(\binom{p^n}{l_1}) = e_p(\binom{p^n}{l_2})$, *where* $1 \leq l_1, l_2 \leq p-1$ *and* $n \in \mathbb{N}$.
Moreover, $e_p(\binom{p^n}{l_1}) = n$.

Lemma 2

Lemma

Let $a \geq 2$, *and* $s, n \in \mathbb{N}$, *where* $p^{s-1} < a \leq p^s$. *For,* $0 \leq i \leq s-2$, $1 \leq k \leq (p-1)p^{s-2-i} - 1$. *Then:*

1. $e_p(\binom{p^{s+n-1}}{p^{s-1-i}}) \geq n$.
2. $e_p(\binom{p^{s+n-1}}{p^{s-1-i}+l_1}) = e_p(\binom{p^{s+n-1}}{p^{s-1-i}+l_2})$, *where* $1 \leq l_1, l_2 \leq p-1$. *Moreover,* $e_p(\binom{p^{s+n-1}}{p^{s-1-i}+l_1}) \geq n$.
3. $e_p(\binom{p^{s+n-1}}{p^{s-1-i}+kp}) \geq n$.
4. $e_p(\binom{p^{s+n-1}}{p^{s-1-i}+kp+l_1}) = e_p(\binom{p^{s+n-1}}{p^{s-1-i}+kp+l_2})$, *where* $1 \leq l_1, l_2 \leq p-1$. *Moreover,* $e_p(\binom{p^{s+n-1}}{p^{s-1-i}+kp+l_1}) \geq n$.

Lemmas 3–4

Lemma

Let $a \geq 2$, and $s, n \in \mathbb{N}$, where $p^{s-1} < a \leq p^s$. Let $f(x)$ be a monic polynomial in $GR(p^n, d)[x]$ such that the reduction $\overline{f}(x)$ in $\mathbb{F}_{p^d}[x]$ is irreducible. Then:

1. $e_p(\binom{p^{s+n-1-t}}{p^{s-1}}) = n - t$ *for all* $t \in \mathbb{N}$.
2. $(1 + f(x) + (f(x)^a))^{p^{s+n-1-t}} \neq 1 + (f(x)^a)$ *for all* $t \in \mathbb{N}$.

Lemma

$e_p(m!) < \frac{m}{p-1}$ *for all* $m \in \mathbb{N}$.

Now, we are ready to compute the exponent of $GR(p^n, d)[x]/(f(x)^a)$, when $a \geq 2$.

Theorem

Let $f(x) \in GR(p^n, d)[x]$ be a monic polynomial of degree r such that the reduction $\overline{f}(x)$ in $\mathbb{F}_{p^d}[x]$ is irreducible, and $a \geq 2$. If s is the positive integer such that $p^{s-1} < a \leq p^s$, then

$$\lambda(GR(p^n, d)[x]/(f(x)^a)) = p^{s+n-1}(p^{dr} - 1).$$

Proof

Let $h(x) \in pGR(p^n, d)[x]$, and $l(x) \in GR(p^n, d)[x]$, where $\deg h < r$, and $\deg l < r(a-1)$. Then

$$\begin{aligned}(1+h+fl+(f^a))^{p^{s+n-1}} &= (1+fl)^{p^{s+n-1}} + \binom{p^{s+n-1}}{1}(1+fl)^{p^{s+n-1}-1}h \\ &+ \cdots + \binom{p^{s+n-1}}{p^{s+n-1}-1}(1+fl)h^{p^{s+n-1}-1} \\ &+ h^{p^{s+n-1}} + (f^a).\end{aligned}$$

Proof

Since $h(x) \in pGR(p^n, d)[x]$, Lemma 4 forces that

$$\binom{p^{s+n-1}}{1} h = \cdots = \binom{p^{s+n-1}}{p^{s+n-1}-1} h^{p^{s+n-1}-1} = h^{p^{s+n-1}} = 0.$$

Thus,

$$\begin{aligned}(1 + h + fl + (f^a))^{p^{s+n-1}} &= (1 + fl)^{p^{s+n-1}} + (f^a) \\ &= 1 + \binom{p^{s+n-1}}{1} fl + \cdots + \binom{p^{s+n-1}}{p^{s-1}} (fl)^{p^{s-1}} \\ &\quad + \cdots + \binom{p^{s+n-1}}{a-1} (fl)^{a-1} + (f^a).\end{aligned}$$

Lemmas 1 and 2 imply that $p^n \mid \binom{p^{s+n-1}}{i}$ for all i.

Hence, $(1 + h + fl + (f^a))^{p^{s+n-1}} = 1 + (f^a)$.

Proof

Thus, Lemma 3 implies that p^{s+n-1} is the order of $1+f+(f^a) \in 1+M$, so $\exp(1+M) = p^{s+n-1}$.

Therefore,

$$\begin{aligned} \lambda(GR(p^n,d)[x]/(f(x)^a)) &= \mathrm{lcm}(\exp(1+M), \exp \mathbb{F}_{p^{dr}}^{\times}) \\ &= p^{s+n-1}(p^{dr}-1) \end{aligned}$$

as desired. □

Meemark Y., Tocharoenirattisai I.: Exponent of local ring extension of Galois rings and digraphs of the kth power mapping, *Turk. J. Math.*, to appear.

The End

http://pioneer.netserv.chula.ac.th/~myotsana/