Revista Integración
ISSN: 0120-419X
ISSN: 2145-8472
Universidad Industrial de Santander

KIRIU, YUKI; MEJÍA, DIEGO A.
Some notes about power residues modulo prime
Revista Integración, vol. 40, no. 1, 2022, January-June, pp. 1-23
Universidad Industrial de Santander

DOI: https://doi.org/10.18273/revint.v40n1-2022001

Available in: https://www.redalyc.org/articulo.oa?id=327072449001

Revista Integración
Escuela de Matemáticas
Universidad Industrial de Santander
Vol. 40, No. 1, 2022, pág. 1–23

Some notes about power residues modulo prime

Yuki Kiriu [a], Diego A. Mejía [b] ✉,

[a] Shizuoka Salesio High School, Shizuoka, Japan.

[b] Shizuoka University, Faculty of Science, Creative Science Course (Mathematics), Shizuoka, Japan.

Abstract. Let q be a prime. We classify the odd primes $p \neq q$ such that the equation $x^2 \equiv q \pmod{p}$ has a solution, concretely, we find a subgroup $\mathbb{L}_{4q}$ of the multiplicative group $\mathbb{U}_{4q}$ of integers relatively prime with $4q$ (modulo $4q$) such that $x^2 \equiv q \pmod{p}$ has a solution iff $p \equiv c \pmod{4q}$ for some $c \in \mathbb{L}_{4q}$. Moreover, $\mathbb{L}_{4q}$ is the only subgroup of $\mathbb{U}_{4q}$ of half order containing -1.

Considering the ring $\mathbb{Z}[\sqrt{2}]$, for any odd prime p it is known that the equation $x^2 \equiv 2 \pmod{p}$ has a solution iff the equation $x^2 - 2y^2 = p$ has a solution in the integers. We ask whether this can be extended in the context of $\mathbb{Z}[\sqrt[n]{2}]$ with $n \geq 2$, namely: for any prime $p \equiv 1 \pmod{n}$, is it true that $x^n \equiv 2 \pmod{p}$ has a solution iff the equation $D_n^2(x_0, \ldots, x_{n-1}) = p$ has a solution in the integers? Here $D_n^2(\bar{x})$ represents the norm of the field extension $\mathbb{Q}(\sqrt[n]{2})$ of $\mathbb{Q}$. We solve some weak versions of this problem, where equality with p is replaced by $0 \pmod{p}$ (divisible by p), and the "norm" $D_n^r(\bar{x})$ is considered for any $r \in \mathbb{Z}$ in the place of 2.

Keywords: Power residues modulo prime, quadratic residues, Legendre symbol, norms of field extensions, irreducible polynomials.

MSC2010: 11A15, 11C20, 11R04.

Sobre residuos de potencias módulo primo

Resumen. Sea q un número primo. Clasificamos los primos impares $p \neq q$ tal que la ecuación $x^2 \equiv q \pmod{p}$ tiene solución, concretamente, hay un subgrupo $\mathbb{L}_{4q}$ del grupo multiplicativo $\mathbb{U}_{4q}$ de los enteros primos relativos con $4q$ (módulo $4q$) tal que $x^2 \equiv q \pmod{p}$ tiene solución si y solo si $p \equiv c \pmod{4q}$ para algún $c \in \mathbb{L}_{4q}$. Aún más, $\mathbb{L}_{4q}$ es el único subgrupo de $\mathbb{U}_{4q}$ con la mitad del orden que contiene a -1.

En conexión con el anillo $\mathbb{Z}[\sqrt{2}]$, para cualquier primo impar p se sabe que la ecuación $x^2 \equiv 2 \pmod{p}$ tiene solución si y solo si $x^2 - 2y^2 = p$ tiene solución en los enteros. Nos preguntamos si esta situación se puede extender al

Email: [a]uki_sal@yahoo.co.jp; [b]diego.mejia@shizuoka.ac.jp.✉
Received: 18 March 2021, Accepted: 29 September 2021.
To cite this article: Y. Kiriu and D.A. Mejía, Some notes about power residues modulo prime, *Rev. Integr. temas mat.*, 40 (2022), No. 1, 1-23. doi: 10.18273/revint.v40n1-2022001

contexto de $\mathbb{Z}[\sqrt[n]{2}]$ con $n \geq 2$, a saber: para cualquier primo $p \equiv 1 \pmod{n}$, ¿la ecuación $x^n \equiv 2 \pmod{p}$ tiene solución si y solo si $D_n^2(x_0, \ldots, x_{n-1}) = p$ tiene solución en los enteros? Aquí $D_n^2(\bar{x})$ representa la norma de $\mathbb{Q}(\sqrt[n]{2})$ como extensión del campo $\mathbb{Q}$. Solucionamos algunas versiones débiles de este problema, donde igualdad con p se reemplaza por 0 (mód p) (divisible por p), y la "norma" $D_n^r(\bar{x})$ se considera para cualquier $r \in \mathbb{Z}$ en lugar de 2.

Palabras clave: Residuos de potencias módulo primo, residuos cuadráticos, símbolo de Legendre, normas de extensiones de campos, polinomios irreducibles.

1. Introduction

In this work, we prove several properties and present problems related with quadratic residues and its generalization to n-th power residues modulo prime, all in the framework of elementary number theory.

Before entering into the subject, we first fix some basic notations.

Notation 1.1. In the following, $m > 1$ is an integer and q is a prime.

(1) $\mathbb{F}_q$ denotes the field of integers modulo q, which is the prime field of order q, and $\mathbb{F}_q^\times$ denotes its associated multiplicative group.

(2) More generally, $\mathbb{U}_m$ denotes the multiplicative group of integers modulo m that are relatively prime with m. Note that $\mathbb{U}_q = \mathbb{F}_q^\times$.

(3) Let G be a group with identity element 1_G. For any $r \in G$, the *order of r in G*, which we denote by $O_G(r)$, is the smallest positive integer n satisfying $r^n = 1_G$ in case it exists, otherwise $O_G(r)$ is *infinite*. When $G = \mathbb{U}_m$, for $r \in \mathbb{U}_m$ we abbreviate $O_m(r) := O_{\mathbb{U}_m}(r)$, which is the smallest positive integer n such that $r^n \equiv 1 \pmod{m}$ (which always exists because $\mathbb{U}_m$ is finite). We can of course extend this notion for any $r \in \mathbb{Z}$ that is relatively prime with m, so $O_m(r) = O_m(r_0)$ where r_0 is the residue obtained after dividing r by m.

(4) The number of elements of a set A is denoted by $\#A$. When G is a group, $\#G$ is also called the *order of G*. When G is a finite group and $r \in G$, $O_G(r)$ divides $\#G$. Therefore, since $\#\mathbb{U}_m = \varphi(m)$ where φ denotes *Euler's phi function*, $O_m(r) \mid \varphi(m)$ for any integer r relatively prime with m. In particular, if q does not divide r then $O_q(r) \mid \varphi(q) = q - 1$.

(5) Let $r \in \mathbb{Z}$ be relatively prime with m. Since $O_m(r) \mid \varphi(m)$, there is a unique (positive) integer $n_m(r)$ satisfying $O_m(r)n_m(r) = \varphi(m)$. Therefore, due to the definition of $O_m(r)$, $n_m(r)$ is the *largest* $n \mid \varphi(m)$ such that $r^{\frac{\varphi(m)}{n}} \equiv 1 \pmod{m}$.

The notion of $n_m(r)$ is not standard, but it will be very useful in the context of power residues modulo prime, as well as in characterizations of $O_m(r)$.

Euler's criterion for quadratic residues modulo prime can be easily generalized to power residues as follows (see e.g. [5, Thm. 3.11], [8, Thm. 1.29] and [3, Prop. 4.2.1]).

Theorem 1.2 (Generalized Euler's criterion)**.** *Let $r \in \mathbb{Z}$, p a prime not dividing r and let n be a positive integer. Then the equation $x^n \equiv r \pmod{p}$ has a solution iff*

$$r^{\frac{p-1}{\gcd(p-1,n)}} \equiv 1 \pmod{p}.$$

Even more, if the equation $x^n \equiv r \pmod{p}$ has a solution then it has $\gcd(p-1,n)$-many incongruent solutions modulo p in total.

As a consequence,

Corollary 1.3. *Let $r \in \mathbb{Z}$ and p a prime not dividing r. Then $n_p(r)$ is the largest $n \mid p-1$ such that r has an n-th root modulo p. Moreover, the following statements are equivalent for any positive integer n:*

(I) $x^n \equiv r \pmod{p}$ *has a solution.*

(II) $r^{\frac{p-1}{\gcd(p-1,n)}} \equiv 1 \pmod{p}$.

(III) $\gcd(p-1,n) \mid n_p(r)$.

Proof. The equivalence (i) $\Leftrightarrow$ (ii) is Theorem 1.2; the equivalence (ii) $\Leftrightarrow$ (iii) can be seen from the definition of $n_p(r)$ (see Notation 1.1(5)). ☑

In this view, $n_p(r)$ plays a very important role in relation with power residues modulo p.

The main results of this paper are divided in two parts, the first about quadratic reciprocity, and the second about power reciprocity modulo prime.

Main results 1: On quadratic residues

Fix $r \in \mathbb{Z}$. When p is an odd prime not dividing r (i.e. $\gcd(p,r) = 1$), whether r is a quadratic residue modulo p is determined by the *Legendre symbol*, which is defined by

$$\left(\frac{r}{p}\right) = \begin{cases} 1 & \text{if the equation } x^2 \equiv r \pmod{p} \text{ has a solution,} \\ -1 & \text{otherwise.} \end{cases} \tag{1.4}$$

In the case $r = 2$, the problem of whether 2 is a quadratic residue modulo an odd prime is already solved.

Theorem 1.5 (See e.g. [1, Thm. 9.6])**.** *If p is an odd prime then $\left(\frac{2}{p}\right) = 1$ iff $p \equiv \pm 1 \pmod{8}$.*

We ask about similar characterizations for any integer r.

Problem 1.6. *Let $r \in \mathbb{Z}$. Is there a positive integer $m(r)$ and a set $L(r) \subseteq \mathbb{U}_{m(r)}$ such that, for any prime p not dividing r, $\left(\frac{r}{p}\right) = 1$ iff the residue of p modulo $m(r)$ is in $L(r)$? If so, can $L(r)$ be characterized in some way?*

The answer to the first question should not be difficult due to the quadratic reciprocity law, but the characterization of $L(r)$ is more interesting for settling the general problem. In fact, due to the property

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right), \tag{1.7}$$

the interesting case of Problem 1.6 is when r is a prime. In this case, we proved the following main result:

Theorem A (Theorem 3.5)**.** *Let q be a prime. Then*

(a) There is only one subgroup of $\mathbb{U}_{4q}$ with order $\frac{\#\mathbb{U}_{4q}}{2}$ containing -1. This subgroup is denoted by $\mathbb{L}_{4q}$.

(b) For any prime $p \neq q$, $\left(\frac{q}{p}\right) = 1$ iff the residue of p modulo $4q$ is in $\mathbb{L}_{4q}$.

This theorem becomes a tool to calculate $\left(\frac{r}{p}\right)$ for any $r \in \mathbb{Z}$ relatively prime with p. This is presented in Theorem 3.6 (and at the end of Section 3).

In the case of composite r, due to Equation (1.7) an extension of Theorem A is reasonable when r is square free. In this case we can find a subgroup $\mathbb{L}_{4r}$ of $\mathbb{U}_{4r}$ containing -1 as in (b), but in general this group is not unique as in (a). Details are presented in Theorem 3.7 and in the discussion that follows it.

Main results 2: On power residues

We aim to generalize the following result to power residues.

Theorem 1.8 (See e.g. [2, Thm. 256] and [9])**.** *Let p be an odd prime. Then the following statements are equivalent.*

(I) The equation $x^2 \equiv 2 \pmod{p}$ has a solution.

(II) The equation $x^2 - 2y^2 = p$ has an integer solution.

This is related to the characterization of irreducible elements of the ring $\mathbb{Z}[\sqrt{2}]$: an odd prime p in $\mathbb{Z}$ is still a prime in $\mathbb{Z}[\sqrt{2}]$ iff the equation $x^2 - 2y^2 = p$ does not have integer solutions (see [2, Thm. 256]). Recall that $x^2 - 2y^2$ is the norm of $x + y\sqrt{2}$ in the field extension $\mathbb{Q}(\sqrt{2})$ of $\mathbb{Q}$.

For any $n \geq 2$, denote by $D_n^2(x_0, \ldots, x_{n-1})$ the norm of $x_0 + x_1 \sqrt[n]{2} + \ldots x_{n-1} \sqrt[n]{2^{n-1}}$ in the field extension $\mathbb{Q}(\sqrt[n]{2})$ of $\mathbb{Q}$. This norm is defined (even in a more general context) in Section 4, but we just state here that $D_n^2(x_0, \ldots, x_{n-1})$ is an integer when $x_0, \ldots, x_{n-1} \in \mathbb{Z}$. So we ask whether Theorem 1.8 can be generalized in the following sense.

Problem 1.9. *Let $n > 2$ and p a prime such that $p \equiv 1 \pmod{n}$. Are the following statements equivalent?*

(1) The equation $x^n \equiv 2 \pmod{p}$ has a solution.

(2) The equation $D_n^2(x_0, \ldots, x_{n-1}) = p$ *has an integer solution.*

The solution of this problem seems to rely on tools in algebraic number theory that would go beyond elementary number theory. In these terms, we managed to solve weaker versions of the problem, where in some of them (2) is replaced by $D_n^2(x_0, \ldots, x_{n-1}) \equiv 0 \pmod{p}$. The trivial solution of this equation is $x_0 = \ldots = x_{n-1} = 0$, so we aim for non-trivial solutions. On the other hand, our results deal with any integer r in place of 2, so we used a general version $D_n^r(x_0, \ldots, x_{n-1})$ of the norm (which is defined in detail in Section 4).

Theorem B (Theorem 5.1)**.** *Let* p *be a prime,* $r \in \mathbb{Z}$, $n \in \mathbb{Z}^+$ *and* $r_0 \in \mathbb{F}_p$ *such that* $r \equiv r_0 \pmod{p}$.

(a) The polynomial $x^n - r_0$ *is irreducible in* $\mathbb{F}_p[x]$ *iff the equation* $D_n^r(x_0, \ldots, x_{n-1}) \equiv 0 \pmod{p}$ *does not have a non-trivial solution in the integers.*

(b) If $n \geq 2$ *and the equation* $x^n \equiv r \pmod{p}$ *has a solution, then* $D_n^r(x_0, \ldots, x_{n-1}) \equiv 0 \pmod{p}$ *has a non-trivial solution in* $\mathbb{Z}^n$ *satisfying* $-p^{\frac{1}{n}} < x_i < p^{\frac{1}{n}}$ *for all* $0 \leq i < n$.

The proof of Theorem B(b) is inspired in the proof of Theorem 1.8 presented in the post [9]. As a consequence, we obtain the following equivalence when n is a prime.

Corollary (Corollary 5.2)**.** *Let* p *and* q *be primes,* $r \in \mathbb{Z}$. *Then the following statements are equivalent:*

(I) $x^q \equiv r \pmod{p}$ *has a solution.*

(II) $D_q^r(x_0, \ldots, x_{n-1}) \equiv 0 \pmod{p}$ *has a non-trivial solution.*

We can also conclude some weakening of the implication (2) $\Rightarrow$ (1) of Problem 1.9, which yields the real implication when n is a prime.

Theorem C (Theorem 5.3)**.** *Assume that* p *is a prime,* $n \geq 2$, $r \in \mathbb{F}_p$ *and* $r_0 \in \mathbb{F}_p$ *such that* $r \equiv r_0 \pmod{p}$. *If the polynomial* $x^n - r_0$ *is irreducible in* $\mathbb{F}_p[x]$ *then* $D_n^r(\bar{x}) = p$ *does not have a solution in the integers.*

In particular, (2) $\Rightarrow$ *(1) of Problem 1.9 is true when* n *is a prime.*

We also present a simple proof of Theorem 1.8 using Theorem B (see Theorem 5.4), where 2 can also be replaced by $r \in \{-2, -1\}$. This shortens the proof in [9] a little bit.

We remark that "$x^n - r$ is irreducible in $\mathbb{F}_p[x]$" is stronger than "$x^n \equiv r \pmod{p}$ does not have a solution". For instance, if $p \in \{7, 17, 23, 31, 41, 47, 71\}$, the equation $x^2 \equiv 2 \pmod{p}$ has a solution, but $x^{p-1} \equiv 2 \pmod{p}$ does not have one. On the other hand, if a_0 is a solution of $x^2 - 2 = 0$ in $\mathbb{F}_p$ then, in $\mathbb{F}_p[x]$:

$$x^{p-1} - 2 = x^{2(\frac{p-1}{2})} - a_0^2 = (x^{\frac{p-1}{2}} - a_0)(x^{\frac{p-1}{2}} + a_0).$$

This means that $x^{p-1} - 2$ is reducible in $\mathbb{F}_p[x]$. More details about irreducibility of $x^n - r$ are presented in Section 4.

We do not have any counter-example for Problem 1.9 even when $x^n - 2$ is reducible in $\mathbb{F}_p[x]$.

Indirect motivation

The motivation of this work is related with the study of Mersenne primes, although we do not present explicit results about them. A *Mersenne number* is an integer of the form $2^n - 1$ with $n \in \mathbb{Z}^+$ (positive integer), and a *Mersenne prime* is a primer number of this form. It is well known that, whenever $2^n - 1$ is a prime, n must be a prime. Another curious fact is that, whenever $2^n - 1$ is a Mersenne prime, there is only one (odd) prime p such that $O_p(2) \mid n$, that is, such that $2^n \equiv 1 \pmod{p}$. Even more, since n must be prime, $n = O_p(2)$. The converse situation is interesting: if n is a prime and there is only one prime p such that $O_p(2) \mid n$, then $2^n - 1 = p^e$ for some $e \in \mathbb{Z}^+$. Hence, when $e = 1$, $2^n - 1$ is a Mersenne prime; but if $e > 1$ then p is a *Wieferich prime*, i.e., a prime number p satisfying $2^{p-1} \equiv 1 \pmod{p^2}$. Recall that so far only two Wieferich primes are known, namely 1093 and 3511, and Silverman proved under the abc-conjecture that there are infinitely many non-Wieferich primes [7].

The previous observation indicates that understanding $O_p(2)$ would lead to a better understanding of Mersenne primes and would trigger possible characterizations. On the other hand, since $O_p(2)$ is associated with $n_p(2)$, according to Corollary 1.3 we can discover a lot about $n_p(r)$ in general by studying power residues modulo p.

Concerning $O_p(r)$ for some fixed integer $r > 1$, the pattern of the sequence of $O_p(r)$ for prime p relatively prime with r seems to be very *erratic* [6], but $O_n(r)$ in general can be determined in terms of $O_p(r)$ for prime $p \mid n$, see Theorems 2.1–2.3. In particular, $O_{p^e}(r)$ is deeply related with Wieferich primes (in base r). A more detail discussion is presented in Section 2.

Structure of the paper

Section 2. We discuss some simple aspects related with $O_m(r)$ and $n_p(r)$. In particular, we show expressions of $O_m(r)$ for composite m, and a method to obtain n-th roots of 1 modulo a prime p, in particular $n_p(r)$-th roots of 1. The contents of this section are known and unrelated with the main results, but we present them in accordance with the "indirect motivation" above.

Section 3. This is dedicated to the proof of Theorem A and to further discussions about groups associated with quadratic reciprocity.

Section 4. We present some preliminaries in algebra that are going to be required in the proof of the main results about power residues modulo prime.

Section 5. We prove our main results about power residues modulo prime, in particular Theorems B and C.

Section 6. We discuss research related to this work.

2. Multiplicative order

We first show how the multiplicative order modulo composite numbers can be calculated.

Theorem 2.1 (See e.g. [5, §3.2, Thm. 3.6])**.** *Let p be an odd prime and $r \in \mathbb{Z}$, $r \neq \pm 1$ relatively prime with p. Assume that e_0 is the maximum integer such that $O_{p^{e_0}}(r) = O_p(r)$. Then, for any $e \geq 1$,*

$$O_{p^e}(r) = \begin{cases} O_p(r) & \text{when } e \leq e_0, \\ p^{e-e_0} O_p(r) & \text{otherwise.} \end{cases}$$

The previous result has a deep connection with Wieferich primes. In fact, an odd prime p is a *Wieferich prime in base r* if $p \nmid r$ and $O_{p^2}(r) = O_p(r)$.[1] Very few of these numbers are known for each $r > 1$.

The following is a version of Theorem 2.1 for $p = 2$. The proof is almost the same, so we omit it.

Theorem 2.2. *Assume $r \in \mathbb{Z}$ is odd, $r \neq \pm 1$. If $e_0 \geq 2$ is the maximum integer such that $O_{2^{e_0}}(r) = O_4(r)$ then, for any $e \geq 2$,*

$$O_{2^e}(r) = \begin{cases} O_4(r) & \text{when } e \leq e_0, \\ 2^{e-e_0} O_4(r) & \text{otherwise.} \end{cases}$$

Now we look at the case when $m > 1$ is composite but not a prime power, so we assume that it has prime factorization $m = \prod_{i=1}^{s} p_i^{e_i}$ $(s \geq 2)$.

Theorem 2.3. *When* $\gcd(r, m)$*=1,* $O_m(r) = \operatorname{lcm}(O_{p_1^{e_1}}(r), O_{p_2^{e_2}}(r), \ldots, O_{p_s^{e_s}}(r))$.

Proof. Let us suppose $b := \operatorname{lcm}(O_{p_1^{e_1}}(r), O_{p_2^{e_2}}(r), \ldots, O_{p_s^{e_s}}(r))$. We need to prove the following.

1. $r^b \equiv 1 \pmod{m}$. For any $i \leq s$ we know that $r^{O_{p_i^{e_i}}(r)} \equiv 1 \pmod{p_i^{e_i}}$ and $O_{p_i^{e_i}}(r) \mid b$, so $r^b \equiv 1 \pmod{p_i^{e_i}}$, i.e. $p_i^{e_i} \mid r^b - 1$. Since $p_i^{e_i}$ and $p_j^{e_j}$ are relatively prime when $i \neq j$, we conclude that $m \mid r^b - 1$.

2. *b is the minimal number satisfying the equation $r^x \equiv 1 \pmod{p}$* Assume $r^x \equiv 1 \pmod{m}$. This implies $r^x \equiv 1 \pmod{p_i^{e_i}}$ for any $i \leq s$, so $O_{p_i^{e_i}}(r) \mid x$. Therefore $b \mid x$, so by (1) b is the minimum we claim. ☑

Notice that, by the Chinese remainder theorem, the map $\mathbb{Z}_m \to \bigoplus_{i=1}^{s} \mathbb{Z}_{p_i^{e_i}}$ that sends a to the tuple $(a_1, \ldots, a_s)$ of residues modulo $p_i^{e_i}$ is a ring isomorphism, and when restricted to $\mathbb{U}_m$ it gives a group isomorphism onto $\oplus_{i=1}^{s} \mathbb{U}_{p_i^{e_i}}$. So the previous result can be seen as a particular case of the following fact: *if $G = \bigoplus_{i=1}^{k} G_i$ is a direct sum of groups of finite order and $\bar{a} = (a_1, \ldots, a_k) \in G$, then $O_G(\bar{a}) = \operatorname{lcm}(O_{G_1}(a_1), \ldots, O_{G_k}(a_k))$.* (A similar proof works.)

As a consequence, we obtain the following modular equation using Euler's phi function.

[1] The standard definition is $r^{p-1} \equiv 1 \pmod{p^2}$, which is equivalent thanks to Theorem 2.1: If $O_{p^2}(r) \neq O_p(r)$ then $O_{p^2}(r) = pO_p(r)$, which does not divide $p - 1$.

Corollary 2.4. *If* $\gcd(r,m)=1$ *and*

$$c=\frac{\varphi(m)}{\gcd(\varphi(p_1^{e_1}),\varphi(p_2^{e_2}),\ldots,\varphi(p_s^{e_s}))}$$

then $r^c\equiv 1 \pmod m$.

Proof. Since $\operatorname{lcm}(a_1,a_2,\ldots,a_m)\cdot\gcd(a_1,a_2,\ldots,a_m) \mid a_1a_2\cdots a_m$, by Theorem 2.3 we can prove that

$$\begin{aligned} O_m(r) &\mid \operatorname{lcm}(\varphi({p_1}^{e_1}),\varphi({p_2}^{e_2}),\ldots,\varphi({p_s}^{e_s}))\\ \text{and } \operatorname{lcm}(\varphi({p_1}^{e_1}),\varphi({p_2}^{e_2}),\ldots,\varphi({p_s}^{e_s})) &\mid c. \end{aligned}$$

The theorem follows immediately. ☑

The previous result can be generalized as well in the context of direct sums of groups: *if* $\bar a\in G$ *and* $c=\frac{\#G}{\gcd(\#G_1,\ldots,\#G_k)}$ *then* $\bar a^c=1_G$, *i.e.* $O_G(\bar a)\mid c$.

From here until the end of this section, we assume that p is a prime and $\gcd(r,p)=1$. We look at the effect of the power of $O_p(r)$ in $\mathbb{F}_p^\times$, namely, properties of $k^{O_p(r)}$ for $k\in\mathbb{F}_p$. In fact, these properties come from more general results. First, we show that $\{k^{O_p(r)} : k\in\mathbb{F}_p^\times\}$ gives the full set of $n_p(r)$-th roots of 1 modulo p, which can be generalized as follows.

Theorem 2.5. *Let* $n\geq 1$ *be an integer. Then all the* n*-th roots of unity can be obtained from the set*

$$A:=\left\{a^{\frac{p-1}{\gcd(n,p-1)}} : a\in\mathbb{F}_p^\times\right\}$$

Moreover, if r_p *is a primitive root of* p *then the set above coincides modulo* p *with*

$$B:=\left\{{r_p}^{\ell\frac{p-1}{\gcd(n,p-1)}} : 0\leq\ell<\gcd(n,p-1)\right\},$$

and their members are pairwise incongruent modulo p.

Proof. We define $m(n):=\frac{p-1}{\gcd(n,p-1)}$ and $b:={r_p}^{m(n)}$. For any $a\in\mathbb{F}_p^\times$, if $a\equiv {r_p}^k \pmod p$ then $a^{m(n)}\equiv {r_p}^{km(n)} \pmod p$. If we put $k=d\cdot\gcd(n,p-1)+\ell$ for some $d\in\mathbb{Z}$ and $0\leq\ell<\gcd(n,p-1)$, then $km(n)=d(p-1)+\ell m(n)$. So we get $a^{m(n)}\equiv\left({r_p}^{m(n)}\right)^\ell\equiv b^\ell \pmod p$. This shows $A\subseteq B$ (modulo p). The converse inclusion is trivial.

By Theorem 1.2, the equation $x^n\equiv 1 \pmod p$ has exactly $\gcd(n,p-1)$-many solutions in $\mathbb{F}_p$. On the other hand, since $O_p(b)=\gcd(n,p-1)$, it is clear that $\left(b^\ell\right)^n\equiv 1 \pmod p$ for all $0\leq\ell<\gcd(n,p-1)$, and that the b^ℓ are pairwise incongruent modulo p. This shows that B is the complete set of n-th roots of unity. ☑

Corollary 2.6. *The set of solutions for the equation* $x^{n_p(r)}\equiv 1 \pmod p$ *(i.e. the set of* $n_p(r)$*-th roots of unity modulo* p*) is*

$$\left\{a^{O_p(r)} : a\in\mathbb{F}_p^\times\right\}=\left\{{r_p}^{\ell O_p(r)} : 0\leq\ell<n_p(r)\right\} \text{ (modulo } p).$$

Recall the following properties of roots of unity modulo p.

Lemma 2.7. *Let $n \geq 1$ and assume that a is an n-th root of 1 modulo p. Then:*

(a) If $a \equiv 1 \pmod{p}$ then $\sum_{i=0}^{n-1} a^i \equiv n \pmod{p}$.

(b) If $a \not\equiv 1 \pmod{p}$ then $\sum_{i=0}^{n-1} a^i \equiv 0 \pmod{p}$.

Proof. Property (a) is trivial; since

$$(a-1)\sum_{i=0}^{n-1} a^i = a^n - 1 \equiv 0 \pmod{p},$$

it is clear that $a \not\equiv 1 \pmod{p}$ implies (b). ☑

As a consequence, we can show the behaviour of the sum of $k^{O_p(r)}$ for $1 \leq k \leq p-1$, or even more generally:

Theorem 2.8 (See e.g. [8, Pg. 67])**.** *Let $n \in \mathbb{Z}^+$. Then:*

(a) $p-1 \mid n \Leftrightarrow \sum_{k=1}^{p-1} k^n \equiv p-1 \pmod{p}$.

(b) $p-1 \nmid n \Leftrightarrow \sum_{k=1}^{p-1} k^n \equiv 0 \pmod{p}$.

Proof. Fix a primitive root r_p of p, and for each $1 \leq k < p$ choose $e_k < p-1$ such that ${r_p}^{e_k} \equiv k \pmod{p}$. We have the following:

$$\sum_{k=1}^{p-1} k^n \equiv \sum_{k=1}^{p-1} ({r_p}^{e_k})^n \equiv \sum_{k=1}^{p-1} \left({r_p}^n\right)^{e_k} \equiv \sum_{i=0}^{p-2} \left({r_p}^n\right)^i \pmod{p}.$$

Note that any member of $\mathbb{F}_p^\times$ is a $(p-1)$-th root of 1, so we can apply Lemma 2.7 to conclude:

(a) if ${r_p}^n \equiv 1 \pmod{p}$ then $\sum_{i=0}^{p-2} \left({r_p}^n\right)^i \equiv p-1 \pmod{p}$;

(b) if ${r_p}^n \not\equiv 1 \pmod{p}$ then $\sum_{i=0}^{p-2} \left({r_p}^n\right)^i \equiv 0 \pmod{p}$.

It is easy to verify that ${r_p}^n \equiv 1 \pmod{p}$ is equivalent to $p-1 \mid n$, so the result follows. ☑

Corollary 2.9. *Let $r \in \mathbb{Z}$ such that $\gcd(r,p) = 1$. Then:*

(a) $O_p(r) = p-1 \Leftrightarrow \sum_{k=1}^{p-1} k^{O_p(r)} \equiv p-1 \pmod{p}$.

(b) $O_p(r) \neq p-1 \Leftrightarrow \sum_{k=1}^{p-1} k^{O_p(r)} \equiv 0 \pmod{p}$.

3. Groups associated with quadratic residues

This section is dedicated to the proof of Theorem A.

Recall the Legendre symbol $\left(\frac{r}{p}\right)$ as presented in Equation (1.4). It is known that the map $\mathbb{F}_p^\times \to \mathbb{U}_4$, $r \mapsto \left(\frac{r}{p}\right)$ is a group homomorphism, where $\mathbb{U}_4 = \{1,-1\}$ as a multiplicative group,[2] so

$$\mathbb{L}_p^* := \left\{ a \in \mathbb{F}_p^\times : \left(\frac{a}{p}\right) = 1 \right\} \tag{3.1}$$

is a subgroup of $\mathbb{F}_p^\times$ of order $\frac{p-1}{2}$ (half of the order of $\mathbb{F}_p^\times$).

We look at the following converse situation: given an integer r, characterize the odd primes p relatively prime with r such that $\left(\frac{r}{p}\right) = 1$. This is associated with $n_p(r)$ in the following sense.

Lemma 3.2. *Let p be an odd prime, $r \in \mathbb{Z}$ such that $\gcd(r,p) = 1$. Then the following statements are equivalent:*

(I) $\left(\frac{r}{p}\right) = 1$.

(II) $x^2 \equiv r \pmod{p}$ *has a solution.*

(III) $r^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

(IV) $n_p(r)$ *is even.*

Proof. The equivalence (i) $\Leftrightarrow$ (ii) follows from the definition of Lagrange's symbol. The others are a direct consequence of Corollary 1.3 (applied to $n = 2$). ☑

First, we look at the case when $r = q$ is a prime. If $q = 2$ we have the following situation.

Theorem 3.3. *If p is an odd prime then the following statements are equivalent.*

(I) $\left(\frac{2}{p}\right) = 1$.

(II) $p \equiv \pm 1 \pmod{8}$.

[2] This is isomorphic to the additive group $\mathbb{Z}_2$.

(III) $2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

(IV) $n_p(2)$ *is even.*

Proof. (i) $\Leftrightarrow$ (ii) is known, see Theorem 1.5. The rest follows by Lemma 3.2. ☑

We aim to generalize Theorem 3.3 for any r in the place of 2, concretely, to find a condition like in (ii) that characterizes $\left(\frac{r}{p}\right)$ for any odd prime p relatively prime with r.

An observation about the case $r = 2$: Denote $\mathbb{L}_8 := \{1, -1\}$ as a subgroup of $\mathbb{U}_8$. Note that this is the only subgroup of $\mathbb{U}_8$ of order 2 (half of the order of $\mathbb{U}_8$) that contains -1. Theorem 3.3 says that $\left(\frac{2}{p}\right) = 1$ iff $p \equiv c \pmod 8$ for some $c \in \mathbb{L}_8$, which validates Theorem A for $r = 2$.

Assume that $r = q$ is an odd prime. If $p \neq q$ is an odd prime then, by the quadratic reciprocity law:

$$\left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}} \left(\frac{p}{q}\right). \tag{3.4}$$

We start assuming $q \equiv -1 \pmod 4$,[3] in which case

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right).$$

Therefore, $\left(\frac{q}{p}\right) = 1$ iff one of the following cases hold:

(I) $p \equiv 1 \pmod 4$ and $p \equiv a \pmod q$ for some $a \in \mathbb{L}_q^*$ (see Equation (3.1)), or

(II) $p \equiv -1 \pmod 4$ and $p \equiv b \pmod q$ for some $b \in \mathbb{U}_q \smallsetminus \mathbb{L}_q^*$.

For any odd prime q_0: by the Chinese remainder theorem, the map $F_{q_0} : \mathbb{Z}_{4q_0} \to \mathbb{Z}_4 \oplus \mathbb{F}_{q_0}$ that sends any x to the pair (x_0, x_1) of remainders modulo 4 and q_0 respectively, is a ring isomorphism. When this map is restricted to $\mathbb{U}_{4q_0}$ it becomes a group isomorphism onto $\mathbb{U}_4 \oplus \mathbb{F}_{q_0}^\times$.

Coming back to our argument, using the previous terminology we conclude that $\left(\frac{q}{p}\right) = 1$ iff $p \equiv c \pmod{4q}$ for some $c \in \mathbb{U}_{4q_0}$ such that c satisfies one of the following conditions:

$(\star)_1^q$: $F_q(c) = (1, a)$ for some $a \in \mathbb{L}_q^*$ (by (i)), or

$(\star)_2^q$: $F_q(c) = (-1, b)$ for some $b \in \mathbb{U}_q \smallsetminus \mathbb{L}_q^*$ (by (ii)).

Let $\mathbb{L}_{4q}$ be the set of $c \in \mathbb{U}_{4q}$ satisfying either $(\star)_1^q$ or $(\star)_2^q$. Since

$$L'_{(4,q)} := \{(e, a) \in \mathbb{U}_4 \oplus \mathbb{U}_q : \text{either } e = 1 \text{ and } a \in \mathbb{L}_q^*, \text{ or } e \neq 1 \text{ and } a \notin \mathbb{L}_q^*\}$$

[3] Although the easy case is $q \equiv 1 \pmod 4$, we decided to start with the other case for convenience of the presentation.

is a subgroup of $\mathbb{U}_4 \oplus \mathbb{U}_q$ and $\mathbb{L}_{4q}$ is the inverse image under F_q of this subgroup, we conclude that $\mathbb{L}_{4q}$ is a subgroup of $\mathbb{U}_{4q}$.

Moreover, $\mathbb{L}_{4q}$ has order $q-1$, which is half of the order of $\mathbb{U}_{4q}$, and $-1 \in \mathbb{L}_{4q}$: Since $\mathbb{L}_q^*$ has order $\frac{q-1}{2}$, it is clear that the order of $L'_{(4,q)}$ is double, that is, $q-1$, and this is the order of $\mathbb{L}_{4q}$; note that $F_q(-1) = (-1,-1)$ and $-1 \notin \mathbb{L}_q^*$ because $q \equiv -1 \pmod 4$, so it satisfies $(\star)_2^q$ and we get $-1 \in \mathbb{L}_{4q}$.

We turn to the case when $q \equiv 1 \pmod 4$. By Equation (3.4) we obtain that $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$, so $\left(\frac{q}{p}\right) = 1$ iff $p \equiv a \pmod q$ for some $a \in \mathbb{L}_q^*$. Using the ring isomorphism F_q introduced before, define

$$\mathbb{L}_{4q} := \{c \in \mathbb{U}_{4q} : F_q(c) = (e,a) \text{ for some } e \in \mathbb{U}_4 \text{ and } a \in \mathbb{L}_q^*\}.$$

Since this is the inverse image under F_q of $\mathbb{U}_4 \oplus \mathbb{L}_q^*$ and this is a subgroup of $\mathbb{U}_4 \oplus \mathbb{U}_q$ of size $q-1$, we conclude that $\mathbb{L}_{4q}$ is a subgroup of $\mathbb{U}_{4q}$ of order $q-1$ (half of the order of $\mathbb{U}_{4q}$). Even more, $-1 \in \mathbb{L}_{4q}$ because $F_q(-1) = (-1,-1)$ and, since $q \equiv 1 \pmod 4$, $-1 \in \mathbb{L}_q^*$.

The previous argument is then summarized in the following result, which generalizes Theorem 3.3 and concludes the proof of Theorem A.

Theorem 3.5. *Let $q \neq p$ be prime numbers with p odd. Then $\left(\frac{q}{p}\right) = 1$ iff $p \equiv c \pmod{4q}$ for some $c \in \mathbb{L}_{4q}$.*

Moreover, $\mathbb{L}_{4q}$ is the unique subgroup of $\mathbb{U}_{4q}$ with order $q-1$ (half of the order of $\mathbb{U}_{4q}$) that contains -1.

Proof. According to the previous discussion, it remains to show that, whenever q is an odd prime, $\mathbb{L}_{4q}$ is the unique subgroup of $\mathbb{U}_{4q}$ as in the statement. So let G be a subgroup of $\mathbb{U}_{4q}$ of order $q-1$ with $-1 \in G$. This indicates that $(-1) := \{1,-1\}$ is a subgroup of G, so when taking quotients

$$\mathbb{U}_{4q}/G \cong (\mathbb{U}_{4q}/(-1))/(G/(-1)).$$

Note that $\mathbb{U}_{4q}/(-1) \cong \mathbb{U}_{2q}$ and $G/(-1)$ is a subgroup of $\mathbb{U}_{4q}/(-1)$ of order $\frac{q-1}{2}$. So it is enough to show that $\mathbb{U}_{2q}$ contains only one subgroup of order $\frac{q-1}{2}$.

By the Chinese remainder theorem, $\mathbb{U}_{2q}$ is isomorphic to $\mathbb{U}_2 \oplus \mathbb{F}_q^\times$, which is isomorphic to $\mathbb{F}_q^\times$ itself. Since $\mathbb{F}_q^\times$ is a cyclic group, it only contains one subgroup of order $\frac{q-1}{2}$, which concludes the proof. ☑

Now we turn to the more general case $r \in \mathbb{Z}^+$. If r is a square then trivially $\left(\frac{r}{p}\right) = 1$ for any odd prime p relatively prime with r; if $r = \prod_{i=1}^s q_i^{e_i}$ is the prime factorization of r and r is not a square, and p is an odd prime relatively prime with r, then by (1.7):

$$\left(\frac{r}{p}\right) = \prod_{i=1}^s \left(\frac{q_i}{p}\right)^{e_i} = \prod_{i \in S} \left(\frac{q_i}{p}\right) = \left(\frac{\prod_{i \in S} q_i}{p}\right)$$

where $S := \{i : e_i \text{ is odd}\}$.

Therefore, the general case reduces to when r is square free, that is, it has its prime factorization of the form $q_1 \cdots q_m$ (when all prime powers are 1). Since

$$\left(\frac{r}{p}\right) = \prod_{i=1}^{m} \left(\frac{q_i}{p}\right)$$

we obtain that $\left(\frac{r}{p}\right) = 1$ iff the number of elements of the set $\left\{i : \left(\frac{q_i}{p}\right) = -1\right\}$ is even. We can express this in terms of the groups $\mathbb{L}_{4q}$ thanks to Theorem 3.5.

Theorem 3.6. *Let $r \in \mathbb{Z}^+$.*

(a) If r is a square then $\left(\frac{r}{p}\right) = 1$ for any odd prime p with $\gcd(p, r) = 1$.

(b) Assume that r is not a square and $r = \prod_{i=1}^{s} q_i^{e_i}$ is its prime factorization. If $S := \{i : e_i \text{ is odd}\}$ then, for any odd prime p with $\gcd(p, r) = 1$, $\left(\frac{r}{p}\right) = 1$ iff the number of elements of the set

$$\{i \in S : p \equiv b \pmod{q_i} \text{ for some } b \in \mathbb{U}_{4q_i} \setminus \mathbb{L}_{4q_i}\}$$

is even.

We develop the case $r = q_1 \cdots q_m$ (prime factorization) a bit more. Consider the ring homomorphism $F'_r : \mathbb{Z} \to \bigoplus_{i=1}^{m} \mathbb{Z}_{4q_i}$ that sends x to the tuple $(x_1, \ldots, x_m)$ where $x \equiv x_i \pmod{4q_i}$ for any i. Although the kernel of this map is $(4r)\mathbb{Z}$, the image is not everything: as a consequence of the Chinese remainder theorem (for non-coprime moduli),[4]

$$F'_r[\mathbb{Z}] = \left\{(x_1, \ldots, x_m) \in \bigoplus_{i=1}^{m} \mathbb{Z}_{4q_i} : x_i \equiv x_j \pmod 4 \text{ for all } i, j\right\}.$$

Therefore, the map $F_r : \mathbb{Z}_{4r} \to F'_r[\mathbb{Z}]$ defined by $F_r(a) = F'_r(a)$, is a ring isomorphism. If we restrict this map to $\mathbb{U}_{4r}$, we get a group isomorphism onto

$$U'_{(4,r)} := F'_r[\mathbb{Z}] \cap \bigoplus_{i=1}^{m} \mathbb{U}_{4q_i} = \left\{(x_1, \ldots, x_m) \in \bigoplus_{i=1}^{m} \mathbb{U}_{4q_i} : x_i \equiv x_j \pmod 4 \text{ for all } i, j\right\}.$$

According to (b), define

$$L'_{(4,r)} := \{(x_1, \ldots, x_m) \in U'_{(4,r)} : \text{the number of elements of the set } \{i : x_i \in \mathbb{U}_{4q_i} \setminus \mathbb{L}_{4q_i}\} \text{ is even}\}.$$

And let $\mathbb{L}_{4r} = \{x \in \mathbb{U}_{4r} : F_r(x) \in L'_{(4,r)}\}$. Therefore, for any odd prime p with $\gcd(p, r) = 1$, $\left(\frac{r}{p}\right) = 1$ iff $p \equiv c \pmod{4r}$ for some $c \in \mathbb{L}_{4r}$.

[4]This holds even when some q_i is 2. Recall that the Chinese remainder theorem (for non-coprime moduli) states that a system of congruences $x \equiv a_i \pmod{n_i}$ $(1 \le i \le m)$ has a solution iff $a_i \equiv a_j \pmod{\gcd(n_i, n_j)}$ for all i, j, and the solution (if it exists) is unique modulo $\operatorname{lcm}(n_1, \ldots, n_m)$ (this is a generalization of [5, §2.4, Thm. 2.9] that can be easily proved by induction).

It is easy to check that $L'_{(4,r)}$ is a subgroup of $U'_{(4,r)}$ of half order, so $\mathbb{L}_{4r}$ is a subgroup of $\mathbb{U}_{4r}$ of half order. Moreover, $-1 \in \mathbb{L}_{4r}$ because $\{i : -1 \in \mathbb{U}_{4q_i} \smallsetminus \mathbb{L}_{4q_i}\}$ is empty by Theorem 3.5 (so it has zero elements). To summarize:

Theorem 3.7. *Let $r \in \mathbb{Z}^+$ with prime factorization $r = q_1 \cdots q_m$. Then there is a subgroup $\mathbb{L}_{4r}$ of $\mathbb{U}_{4r}$ of half order, containing -1, such that for any odd prime p with $\gcd(p,r) = 1$, $\left(\frac{r}{p}\right) = 1$ iff $p \equiv c \pmod{4r}$ for some $c \in \mathbb{L}_{4r}$.*

However, it may be that $\mathbb{L}_{4r}$ is not the only subgroup of $\mathbb{U}_{4r}$ of half order containing -1. For example, consider $r = 15$: $\mathbb{L}_{60} = \{\pm 1, \pm 7, \pm 11, \pm 17\}$, but $\{\pm 1, \pm 11, \pm 19, \pm 29\}$ is another subgroup of $\mathbb{U}_{60}$ of half order containing -1.

To finish this section, we consider negative integers. If $r \in \mathbb{Z}^+$ and p is an odd prime with $\gcd(r,p) = 1$ then

$$\left(\frac{-r}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{r}{p}\right).$$

Since $\left(\frac{-1}{p}\right) = 1$ iff $p \equiv 1 \pmod 4$, $\left(\frac{-r}{p}\right)$ can be easily calculated by Theorem 3.6.

4. Preliminaries about modules and fields

Throughout this section, we fix an arbitrary integral domain R, $r \in R$ and a natural number n. We first discuss the ring quotient $R_n^r := R[x]/(x^n - r)$. It is very common to look at this ring quotient when R is a field and $x^n - r$ is irreducible in $R[x]$, in which case R_n^r is a field. But in this work we also want to look at the situation when $x^n - r$ is reducible in $R[x]$, in which case R_n^r is not an integral domain. In any case:

Lemma 4.1. *The ring R_n^r is a free R-module with basis $\{1, u, \ldots, u^{n-1}\}$ where $u := x \pmod{(x^n - r)}$, even more R_n^r is an R-algebra.*

Proof. Recall that $R[x]$ satisfies the *division algorithm with monic polynomials*: for any $f(x), g(x) \in R[x]$, if $g(x)$ is of the form $x^m + a_{m-1}x^{m-1} + \ldots + a_0$ ($m = 0$ is allowed, in which case $g(x) = 1$) then there are unique $q(x), t(x) \in R[x]$ such that $f(x) = q(x)g(x) + t(x)$ and $t(x)$ has degree smaller than $g(x)$.

Now, if $0 \neq f(x) \in R[x]$ has degree smaller than n then, by applying the previous division algorithm to $g(x) = x^n - r$, we obtain that $f(x) = q(x)g(x) + t(x)$ for unique $q(x)$ and $t(x)$, the latter with degree smaller than n. Hence $q(x) = 0$: if $q(x) \neq 0$ has degree $m \geq 0$, then $q(x)g(x)$, and thus $f(x)$, have degree $n+m$, which contradicts that $f(x)$ has degree smaller than n. Therefore $t(x) = f(x) \neq 0$, meaning that $f(x)$ is not a multiple of $x^n - r$ (otherwise, $t(x) = 0$ by the division algorithm with monic polynomials).

Let R' be the R-submodule of $R[x]$ generated by $\{1, x, \ldots, x^{n-1}\}$, which is a free R-module. The previous paragraph shows that the surjective R-module homomorphism $R' \to R_n^r$ that sends each x^i to u^i has kernel equal to the zero ring, so it is an R-module isomorphism. This shows that R_n^r is a free R-module with basis $\{1, u, \ldots, u^{n-1}\}$.

It is clear that R_n^r is an R-algebra. ☑

If $x^n - r$ is reducible in $R[x]$ then R_n^r is not an integral domain, but it is an integral domain when R is a unique factorization domain and $x^n - r$ is irreducible in $R[x]$. In general, R_n^r can be expressed as a ring of matrices $\mathbb{M}_n^r(R)$ such that the determinant works as the norm of the elements of the ring.

Definition 4.2. (1) For $\bar{x} = (x_0, \ldots, x_{n-1}) \in R^n$ define

$$M_n^r(\bar{x}) := \begin{pmatrix} x_0 & rx_{n-1} & rx_{n-2} & \ldots & rx_2 & rx_1 \\ x_1 & x_0 & rx_{n-1} & \ldots & rx_3 & rx_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ x_{n-2} & x_{n-3} & x_{n-4} & \ldots & x_0 & rx_{n-1} \\ x_{n-1} & x_{n-2} & x_{n-3} & \ldots & x_1 & x_0 \end{pmatrix}$$

and denote its determinant by $D_n^r(\bar{x})$.

(2) If $z \in R_n^r$ we denote $M_n^r(z) := M_n^r(\bar{x})$ and $D_n^r(z) := D_n^r(\bar{x})$ where $\bar{x} = (x_0, \ldots, x_{n-1}) \in R^n$ is the unique tuple such that $z = \sum_{i=0}^{n-1} x_i u^i$.

(3) Define $\mathbb{M}_n^r(R) := \{M_n^r(\bar{x}) : \bar{x} \in R^n\}$. When R is understood from the context we just write $\mathbb{M}_n^r$.

These matrices actually describe the shift endomorphisms in R_n^r:

Lemma 4.3. *If $z \in R_n^r$ then the matrix $M_n^r(z)$ characterizes the endomorphism $R_n^r \to R_n^r$ given by $w \mapsto zw$. Concretely, $M_n^r(z)$ is the unique matrix with the following property: if $w = \sum_{i=0}^{n-1} x_i u^i$ for some $\bar{x} \in R^n$, then $zw = \sum_{i=0}^{n-1} y_i u^i$ where $\bar{y} = M_n^r(z)\bar{x}$.*

As a consequence $\mathbb{M}_n^r$ is a subring of the ring of $n \times n$ matrices with entries in R, even more, $\mathbb{M}_n^r$ is commutative and so it is an R-algebra. In fact, it characterizes R_n^r.

Lemma 4.4. *The function $M_n^r : R_n^r \to \mathbb{M}_n^r$ is an R-algebra isomorphism, and the map $D_n^r : R_n^r \to R$ satisfies $D_n^r(zz') = D_n^r(z)D_n^r(z')$ for any $z, z' \in R_n^r$.*

The function D_n^r has the role of a *norm* for R_n^r. In fact, when F is a field and $x^n - r$ is irreducible in $F[x]$, F_n^r is a field and D_n^r is its norm as an F-extension.

We list the exact form of some few $D_n^r(\bar{x})$ with $\bar{x} \in R^n$:

$$\begin{aligned} D_2^r(\bar{x}) =& {x_0}^2 - {x_1}^2 r; \\ D_3^r(\bar{x}) =& {x_0}^3 + {x_1}^3 r + {x_2}^3 r^2 - 3x_0x_1x_2r; \\ D_4^r(\bar{x}) =& {x_0}^4 - {x_1}^4 r + 4x_0{x_1}^2x_2r - 2{x_0}^2{x_2}^2r - 4{x_0}^2x_1x_3r + {x_2}^4r^2 - 4x_1{x_2}^2x_3r^2 + \\ & 2{x_1}^2{x_3}^2r^2 + 4x_0x_2{x_3}^2r^2 - {x_3}^4r^3. \end{aligned}$$

We can also talk about conjugates in R_n^r. In field extensions like $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$, the conjugate $\bar{z}$ of some element z satisfies that $z\bar{z}$ is the norm of z. In the general case we can look at the matrix characterization: for any matrix A of dimensions $n \times n$ (with entries in R), $A \cdot \mathrm{adj}(A) = |A| I_n$ where I_n is the identity matrix of dimensions $n \times n$, $\mathrm{adj}(A)$ is the *adjugate* of A and $|A|$ is the *determinant* of A. Since the determinant acts as

a norm, then $\mathrm{adj}(A)$ works as the (analog of the) *conjugate* of A. Recall that the matrix A is *invertible* if there is some unique matrix A^{-1} of dimensions $n \times n$, with entries in R, such that $AA^{-1} = A^{-1}A = I_n$. Recall that A is invertible iff $|A|$ is a unit in R, in which case $A^{-1} = |A|^{-1}\mathrm{adj}(A)$. In $\mathbb{M}_n^r(R)$ we obtain:

Lemma 4.5. *If $A \in \mathbb{M}_n^r(R)$ then $\mathrm{adj}(A) \in \mathbb{M}_n^r(R)$. In particular, if $A \in \mathbb{M}_n^r(R)$ is invertible (as a matrix) then $A^{-1} \in \mathbb{M}_n^r(R)$.*

Proof. An analog of the Caley-Hamilton Theorem indicates that

$$(-1)^{n-1}\mathrm{adj}(A) = A^{n-1} + c_{n-1}A^{n-2} + \cdots + c_1 I_n$$

where $c_{n-1}, \ldots, c_0 \in R$ and $\lambda^n + c_{n-1}\lambda^{n-1} + \cdots + c_0$ is the characteristic polynomial of A. If $A \in \mathbb{M}_n^r$ then $(-1)^{n-1}\mathrm{adj}(A) \in \mathbb{M}_n^r$ by the expression above, so $\mathrm{adj}(A) \in \mathbb{M}_n^r$.

In particular, when A is invertible, $A^{-1} = |A|^{-1}\mathrm{adj}(A) \in \mathbb{M}_n^r$.

We also present an elementary proof in the case when $A \in \mathbb{M}_n^r(R)$ is invertible as a matrix with entries in F, where F is the field of fractions of R. Choose $z \in R$ such that $A = M_n^r(z)$. Since A is invertible, by Lemma 4.3 the map $w \mapsto zw$ is an automorphism on F_n^r, so there is some $z' \in F$ such that $zz' = 1$, hence $w \mapsto z'w$ is the inverse of the previous map. Therefore $A^{-1} = M_n^r(z') \in \mathbb{M}_n^r(F)$, which implies that $\mathrm{adj}(A) = |A|A^{-1} \in \mathbb{M}_n^r(F)$. But $\mathrm{adj}(A)$ is a matrix with entries in R, so $\mathrm{adj}(A) \in \mathbb{M}_n^r(R)$. ☑

Now that we know a bit more about the structure of R_n^r, we now look at sufficient and necessary conditions for the polynomial $x^n - r$ to be irreducible.

Lemma 4.6. *If $x^n - r$ is irreducible in $R[x]$ then: whenever $q \mid n$ is prime, $x^q - r = 0$ does not have a solution in R.*

Proof. Assume that $q \mid n$ is prime and $x^q - r = 0$ has a solution v in R, that is, $v^q = r$ in R. Then, in $R[x]$,

$$x^n - r = x^{q\frac{n}{q}} - v^q = (x^{\frac{n}{q}} - v)(x^{\frac{n}{q}(q-1)} + \ldots + v^{q-1}),$$

so $x^n - r$ is reducible. ☑

We will prove the converse in some cases of interest by using the following result. From now on, fix a field F and $r \in F$.

Theorem 4.7 (See [4, Ch. VI §9])**.** *The polynomial $x^n - r$ is irreducible in $F[x]$ iff the following two conditions hold.*

(I) If $q \mid n$ is prime then the equation $x^q - r = 0$ does not have a solution in F.

(II) If $4 \mid n$ then the equation $4x^4 + r = 0$ does not have a solution in F.

Proof. The cited reference states and proves that (i) and (ii) implies that $x^n - r$ is irreducible in $F[x]$. The converse implication is true for any ring R and it is easy to prove. Assume that $r \in R$. Lemma 4.6 shows that $x^n - r$ irreducible in $R[x]$ implies (i). To show that (ii) is also implied we prove that, whenever $4 \mid n$ and $4u^4 + r = 0$ for some $u \in R$, $x^n - r$ is reducible in $R[x]$. Since $n = 4k$ for some $k \geq 1$, we get

$$x^n - r = (x^k)^4 + 4u^4 = ((x^2)^k - 2ux^k + 2u^2)((x^2)^k + 2ux^k + 2u^2).$$ ☑

Corollary 4.8. *Let q be a prime and let F be a field. Then $x^q - r = 0$ does not have a solution in F iff $x^q - r$ is irreducible in $F[x]$.*

Condition (ii) can be suppressed when we look at fields of prime characteristic.

Theorem 4.9. *Let p be a prime and assume that $4 \nmid n$ or $4 \mid p-1$ or $p = 2$. If F has characteristic p then $x^n - r$ is irreducible in $F[x]$ iff, for any prime $q \mid n$, $x^q - r = 0$ does not have a solution in F.*

Proof. We showed one direction in Lemma 4.6. To see the converse, assume that, for any prime $q \mid n$, $x^q - r = 0$ does not have a solution in F, which means that (i) of Theorem 4.7 is valid. By using the same theorem, it is enough to show that (ii) holds, that is, the equation $4x^4 + r = 0$ does not have a solution in F when $4 \mid n$.

Assume that $4 \mid n$, so either $4 \mid p-1$ or $p = 2$ by hypothesis. In the case $4 \mid p-1$ assume towards a contradiction that $4x^4 + r = 0$ has a solution $x_0 \in F$. So $-r = 4x_0^4 = (2x_0^2)^2$. Let $y_0 := 2x_0^2$, so $y_0^2 = -r$.

On the other hand, by properties of the Legendre symbol,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1 \text{ (because } 4 \mid p-1),$$

which means that $-1 \equiv z_0^2 \pmod{p}$ for some $z_0 \in \mathbb{F}_p$. Hence, $r = (-r)(-1) = (y_0 z_0)^2$, that is, the equation $x^2 - r = 0$ has a solution in F, but this is not true by hypothesis: since 2 is prime and $2 \mid n$, $x^2 - r = 0$ does not have a solution in F.

In the case $p = 2$ we have $4x^4 + r = r$. If $4x^4 + r = 0$ has a solution in F then $r = 0$, but $4 \mid n$ so the hypothesis says that the equation $x^2 = 0$ does not have a solution in F, which is absurd. ☑

Corollary 4.10. *Let p be a prime and assume that $n \mid p-1$. If F has characteristic p then $x^n - r$ is irreducible in $F[x]$ iff, for any prime $q \mid n$, $x^q - r = 0$ does not have a solution in F.*

Proof. Immediate by Theorem 4.9 because $4 \mid n$ implies $4 \mid p-1$ when p is odd. ☑

In some cases, we can also characterize irreducibility of $x^n - r$ in $\mathbb{Q}[x]$.

Theorem 4.11. *Let n be a natural number. If $r \in \mathbb{Q}$ and $r > 0$ then $x^n - r$ is irreducible in $\mathbb{Q}[x]$ iff $x^q - r = 0$ does not have a solution in $\mathbb{Q}$ for any prime $q \mid n$.*

Proof. This is a direct consequence of Theorem 4.7 since condition (ii) there is always satisfied. ☑

The previous result actually applies to any ordered field.

To finish this section, we show that irreducible in $\mathbb{F}_p[x]$ is stronger than irreducible in $\mathbb{Q}[x]$ when $r \in \mathbb{Z}$.

Corollary 4.12. *Let p be a prime, $r \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. If $r \equiv r_0 \pmod{p}$ and $x^n - r_0$ is irreducible in $\mathbb{F}_p[x]$ then $x^n - r$ is irreducible in $\mathbb{Q}[x]$.*

Proof. Assume that $x^n - r_0$ is irreducible in $\mathbb{F}_p[x]$. We first prove that $x^q - r = 0$ does not have a solution in $\mathbb{Q}$ for any prime $q \mid n$. Using Lemma 4.6 with $R = \mathbb{F}_p$, we know that $x^q - r_0 = 0$ does not have a solution in $\mathbb{F}_p$ for any prime $q \mid n$, which implies that the equation $x^q - r = 0$ does not have a solution in $\mathbb{Z}$, so neither in $\mathbb{Q}$: if $a, b \in \mathbb{Z}$ are relative prime, $b > 0$, and $\left(\frac{a}{b}\right)^q - r = 0$, then $a^q = rb^q$, which implies that $b = 1$ (if $b > 1$ then $r = 0$, so $a = 0$ and, since $\gcd(a, b) = 1$, $b = 1$, contradiction), thus $x^q - r$ has a solution in $\mathbb{Z}$.

In the case $r > 0$ the result follows by Theorem 4.11; in the case $n \nmid 4$, the result follows by Theorem 4.7; and when $r = 0$, we must have $n = 1$ (because we assumed $x^n - r_0$ irreducible in $\mathbb{F}_p[x]$) and then $x^n - r = x$ is irreducible in $\mathbb{Q}$.

So it remains to consider the case when $r < 0$ and $n \mid 4$. Here it remains to show that (ii) of Theorem 4.7 holds for $F = \mathbb{Q}$. Towards a contradiction, assume that $4a^4 + r = 0$ for some $a \in \mathbb{Q}$. Since $r \in \mathbb{Z}$ and $a^4 = \frac{-r}{4}$, we must have that $a \in \mathbb{Z}$. Therefore, modulo p we get that $4x^4 + r_0 = 0$ has a solution in $\mathbb{F}_p$, but this contradicts (ii) of Theorem 4.7 for $x^n - r_0$ in $\mathbb{F}_p[x]$. ☑

5. Power residues

In this section we show the main results concerning power residues. We start with Theorem B.

Theorem 5.1. *Let p be a prime, $n \in \mathbb{Z}^+$, $r \in \mathbb{Z}$ and let $r_0 \in \mathbb{F}_p$ such that $r \equiv r_0 \pmod p$.*

(a) The polynomial $x^n - r_0$ is irreducible in $\mathbb{F}_p[x]$ iff the equation $D_n^r(x_0, \ldots, x_{n-1}) \equiv 0 \pmod p$ does not have a non-trivial solution in the integers.

(b) If $x^n - r$ is reducible in $\mathbb{Q}[x]$ then $D_n^r(\bar{x}) = 0$ has a non-trivial solution in the integers.

(c) If $n \geq 2$ and the equation $x^n \equiv r \pmod p$ has a solution, then $D_n^r(x_0, \ldots, x_{n-1}) \equiv 0 \pmod p$ has a non-trivial solution in the integers. Even more, this solution satisfies $-p^{\frac{1}{n}} < x_i < p^{\frac{1}{n}}$ for all $0 \leq i < n$.

Proof. Set $F := \mathbb{F}_p$. We first show (a). Assume that $x^n - r_0$ is irreducible in $F[x]$. Then $F_n^{r_0} = F(u)$ is a field extension of F with $u := \sqrt[n]{r_0}$, which is isomorphic to $\mathbb{M}_n^{r_0}(F)$ by Lemma 4.4. Let $\bar{x} = (x_0, \ldots, x_{n-1}) \neq (0, \ldots, 0)$ with $x_i \in \mathbb{F}_p$ $(0 \leq i < n)$, and set $A := M_n^{r_0}(\bar{x})$. By Lemma 4.5 $A^{-1} \in \mathbb{M}_n^{r_0}$, so $D_n^{r_0}(\bar{x}) \neq 0$ in $\mathbb{F}_p$, that is, $D_n^r(\bar{x}) \not\equiv 0 \pmod p$.

For the converse, assume that $x^n - r_0$ is reducible in $F[x]$. Then $F_n^{r_0}$ is not an integral domain, so there are non-zero $z, w \in F_n^{r_0}$ such that $zw = 0$. Then, by Lemma 4.4, $D_n^r(z) D_n^r(w) \equiv 0 \pmod p$, so either $D_n^r(z) \equiv 0 \pmod p$ or $D_n^r(w) \equiv 0 \pmod p$.

To see (b): if $x^n - r$ is reducible in $\mathbb{Q}[x]$ then there are non-zero $z, w \in \mathbb{Q}_n^r$ such that $zw = 0$. Even more, we can find non-zero vectors $\bar{x}, \bar{y} \in \mathbb{Z}^n$ such that $z'w' = 0$ where $z' = \sum_{i=0}^{n-1} x_i u^i$ and $w' = \sum_{i=0}^{n-1} y_i u^i$ (here u determines the basis of $\mathbb{Q}_n^r$ as a $\mathbb{Q}$-vector space). Therefore $D_n^r(\bar{x}) D_n^r(\bar{y}) = 0$, so $D_n^r(\bar{x}) = 0$ or $D_n^r(\bar{y}) = 0$.

Now we show (c). Assume that $x^n \equiv r \pmod p$ has a solution t, that is, $t^n \equiv r \pmod p$.

Consider the set

$$S := \{x \in \mathbb{Z} : \, 0 \leq x < p^{\frac{1}{n}}\}$$

and let

$$S^n := \{(x_0, \ldots, x_{n-1}) : \, x_i \in S \ (0 \leq i < n)\}.$$

Note that S^n has more than p elements (because $n \geq 2$). Now define the function $f : S^n \to \mathbb{F}_p$ by

$$f(x_0, \ldots, x_{n-1}) \equiv x_0 + x_1 t + \cdots + x_{n-1} t^{n-1} \pmod{p}.$$

Since $\mathbb{F}_p$ has p many elements, S^n has more elements than $\mathbb{F}_p$, so by the pigeonhole principle there are two $(m_0, \ldots, m_{n-1}) \neq (m'_0, \ldots, m'_{n-1})$ in S^n such that $f(m_0, \ldots, m_{n-1}) = f(m'_0, \ldots, m'_{n-1})$. For $0 \leq i < n$ let $a_i := m'_i - m_i$, so

$$f(a_0, \ldots, a_{n-1}) \equiv f(m'_0, \ldots, m'_{n-1}) - f(m_0, \ldots, m_{n-1}) \equiv 0 \pmod{p},$$

$\bar{a} := (a_0, \ldots, a_{n-1}) \neq (0, \ldots, 0)$ and $-p^{\frac{1}{n}} < a_i < p^{\frac{1}{n}}$, We show that $\bar{a}$ is as desired.

We proceed in a similar way as in the proof of (a) first assuming that $x^n - r$ is irreducible in $\mathbb{Q}[x]$. Then $K := \mathbb{Q}_n^r = \mathbb{Q}(v)$ is a field extension of $\mathbb{Q}$ with $v = \sqrt[n]{r}$, and it is isomorphic to $\mathbb{M}_n^r(\mathbb{Q})$ by Lemma 4.4. Set $A := M_n^r(\bar{a})$. Since this matrix is not zero, it is invertible, so $A^{-1} \in \mathbb{M}_n^r(\mathbb{Q})$, and even more $B := \operatorname{adj}(A) \in \mathbb{M}_n^r(\mathbb{Z})$ by Lemma 4.5. So choose $\bar{y} \in \mathbb{Z}^n$ such that $B = M_n^r(\bar{y})$.

Since K is $\mathbb{Q}[x]/(q(x))$ with $q(x) := x^n - r$, we have that $A = M_n^r(g(x) \pmod{(q(x))})$ and $B = M_n^r(h(x) \pmod{(q(x))})$ where

$$g(x) := a_0 + a_1 x + \cdots + a_{n-1} x^{n-1},$$
$$h(x) := y_0 + y_1 x + \cdots + y_{n-1} x^{n-1}.$$

Since $AB = |A| I_n$, we get that $x^n - r$ divides $g(x)h(x) - |A|$ in $\mathbb{Q}[x]$, and actually in $\mathbb{Z}[x]$ because both polynomials have coefficients in $\mathbb{Z}$ and $x^n - r$ is monic. Then $g(x)h(x) = j(x)q(x) + |A|$ for some $j(x) \in \mathbb{Z}[x]$.

To finish the proof, note that $g(t)h(t) - |A| = (t^n - r)j(t) \equiv 0 \pmod{p}$, so $g(t)h(t) \equiv |A| \pmod{p}$. On the other hand, we know that $g(t) \equiv f(a_0, \ldots, a_{n-1}) \equiv 0 \pmod{p}$ so $|A| \equiv 0 \pmod{p}$, that is, $D_n^r(a_0, \ldots, a_{n-1}) \equiv 0 \pmod{p}$.

For the general proof of (c) we work in F_n^r, which is isomorphic to $\mathbb{M}_n^r(F)$. Again set $A := M_n^r(\bar{a})$ which is in $M_n^r(F)$, so $B := \operatorname{adj}(A) \in \mathbb{M}_n^r(F)$ by Lemma 4.5. Like above, since $AB = |A| I_n$ we have two polynomials $g(x), h(x) \in F[x]$, which $g(x)$ as above, such that $x^n - r$ divides $g(x)h(x) - |A|$, so $g(x)h(x) = j(x)q(x) + |A|$ for some $j(x) \in F[x]$. Exactly as in the last part of the previous argument, we conclude that $D_n^r(\bar{a}) \equiv 0 \pmod{p}$. ☑

Thanks to the results in Section 4, the previous result takes a simple form when n is a prime.

Corollary 5.2. *Let p and q be primes. Then the equation $x^q \equiv r \pmod{p}$ has a solution iff the equation $D_q^r(x_0, \ldots, x_{n-1}) \equiv 0 \pmod{p}$ has a non-trivial solution.*

Proof. The direction from left to right follows from Theorem 5.1(c). For the converse, if the equation $x^q \equiv r \pmod p$ does not have a solution then the polynomial $x^q - r_0$ is irreducible in $\mathbb{F}_p[x]$ by Corollary 4.8 where $r_0 \in \mathbb{F}_p$ is the residue of r modulo p, so $D_q^r(x_0, \dots, x_{n-1}) \equiv 0 \pmod p$ does not have a non-trivial solution by Theorem 5.1(a). ☑

The next result is Theorem C, which is a weakening of (2) ⇒ (1) of Problem 1.9. This actually checks this implication when n is a prime (for any $r \in \mathbb{Z}$).

Theorem 5.3. *Assume that p is a prime, $r \in \mathbb{Z}$, $r \equiv r_0 \pmod p$ with $r_0 \in \mathbb{F}_p$ and $n \geq 2$. If the polynomial $x^n - r_0$ is irreducible in $\mathbb{F}_p[x]$ then $D_n^r(x_0, \dots, x_{n-1}) = p$ does not have a solution in the integers.*

In particular, if q is a prime and $x^q \equiv r \pmod p$ does not have a solution then $D_q^r(x_0, \dots, x_{q-1}) = p$ does not have a solution in the integers.

Proof. By Theorem 5.1, if $x^n - r_0$ is irreducible in $\mathbb{F}_p[x]$ then $D_n^r(x_0, \dots, x_{n-1}) \equiv 0 \pmod p$ does not have a *non-trivial* solution. Thus, if $D_n^r(x_0, \dots, x_{n-1}) = p$ has a solution $a_0, \dots, a_{n-1} \in \mathbb{Z}$, then every a_i must be a multiple of p. But this implies that $D_n^r(a_0, \dots, a_{n-1})$ is a multiple of p^n, so it cannot be equal to p because $n \geq 2$. ☑

We can use Theorem 5.1 to solve Problem 1.9 for $n = 2$, i.e., Theorem 1.8. In fact, this is valid for -1 and -2 in the place of 2, which yield well known results.

Theorem 5.4. *Let $r \in \{-2, -1, 2\}$. If p is a prime then the equation $x^2 \equiv r \pmod p$ has a solution iff the equation $D_2^r(x_0, x_1) = p$ has a solution in the integers.*

Proof. One implication follows by Theorem 5.3 because 2 is prime. So we show that, whenever $x^2 \equiv r \pmod p$ has a solution, the equation $D_2^r(x_0, x_1) = p$ has a solution in the integers, for $r \in \{-2, -1, 2\}$.

By Corollary 5.2, the equation $D_2^r(x_0, x_1) \equiv 0 \pmod p$ has a non-trivial solution (a, b). Hence p divides $D_2^r(a, b) = a^2 - b^2 r$. According to Theorem 5.1(c), we can find a and b between $-p^{\frac{1}{2}}$ and $p^{\frac{1}{2}}$.

Case $r = 2$. We claim that $-2p < a^2 - 2b^2 < p$. Two cases: if $a^2 \geq 2b^2$ then $0 \leq a^2 - 2b^2 \leq a^2 < p$; if $a^2 < 2b^2$ then $-2p < -2b^2 \leq a^2 - 2b^2 < 0$, so the claim follows.

Now, since $-2p < D_2^2(a, b) = a^2 - 2b^2 < p$ and $p \mid D_2^2(a, b)$, we must have that $D_2^2(a, b) = -p$ (it can not be zero because p must not divide both a and b).

Note that $D_2^2(1, 1) = 1^2 - 2 \cdot 1^2 = -1$, so

$$p = \begin{vmatrix} a & 2b \\ b & a \end{vmatrix} \cdot \begin{vmatrix} 1 & 2 \\ 1 & 1 \end{vmatrix} = \begin{vmatrix} a + 2b & 2(a + b) \\ a + b & a + 2b \end{vmatrix}$$

Hence $x_0 := a + 2b$ and $x_1 = a + b$ form an integer solution of $D_2^2(x_0, x_1) = p$.

Case $r = -1$. It is clear that $0 < a^2 + b^2 < 2p$, so $a^2 + b^2 = p$.

Case $r = -2$. Note that $0 < a^2 + 2b^2 < 3p$, so either $a^2 + 2b^2 = p$ or $a^2 + 2b^2 = 2p$. In the first case we are done; in the second case a must be even, so $a = 2a_0$ for some $a_0 \in \mathbb{Z}$, and $2p = a^2 + 2b^2 = 4a_0^2 + 2b^2$, hence $D_2^{-2}(b, a_0) = p$. ☑

6. Discussions

Problem 1.9 cannot be generalized by simply replacing 2 by any $r \in \mathbb{Z}$. For $n = 2$, it is known it is fine for $r \in \{-2, -1, 2\}$ as shown in Theorem 5.4, but other values of r are problematic. For example, $3y^2 + p$ is never a square when $p \equiv 3 \pmod 4$ (because it is 3 or 2 modulo 4), so $D_2^3(x, y) = p$ does not have a solution for those p. However, there are primes $p \equiv 3 \pmod 4$ such that $x^2 \equiv 3 \pmod p$ has a solution, for example, $p = 11$. In this case, it could be conjectured that the equation $D_2^3(x, y) = p$ has a solution iff $x^2 \equiv 3 \pmod p$ has a solution and $p \equiv 1 \pmod 4$. This motivates:

Problem 6.1. *For $n \geq 2$ (particularly $n = 2$) and $r \in \mathbb{Z}$ (or just free of n-powers), what are suitable necessary and sufficient conditions for a prime p to get that $D_n^r(\bar{x}) = p$ has a solution in the integers?*

As discussed in the introduction, the solution of Problem 1.9 should be related to the characterization of primes (or irreducible) elements in $\mathbb{Z}[\sqrt[n]{2}]$, which looks very complex for general values of n. In the post [10] it is hinted that Problem 1.9 is true for $n = 3$ by looking at $\mathbb{Z}[\sqrt[3]{2}]$ with tools that we did not deal with in this paper.

Some results of Section 5 can be generalized when $x^n - r$ is replaced by any monic polynomial in $\mathbb{Z}[x]$. If R is an integral domain and $q(x) \in R[x]$ is a monic polynomial of degree $n > 0$, the theory in the first part of Section 4 can be generalized in the context of $R_{q(x)} := R[x]/(q(x))$:

(I) $R_{q(x)}$ is a free R-module (and an R-algebra) with basis $\{1, u, \ldots, u^{n-1}\}$ where $u := x \pmod{(q(x))}$

(II) For any $z \in R_{q(x)}$ there is a unique matrix $M_{q(x)}(z)$ that characterizes the endomorphism $R_{q(x)} \to R_{q(x)}$, $w \mapsto zw$ as in Lemma 4.3.

(III) Set $\mathbb{M}_{q(x)} := \mathbb{M}_{q(x)}(R) = \{M_{q(x)}(z) : z \in R_{q(x)}\}$. The function $M_{q(x)} : R_{q(x)} \to \mathbb{M}_{q(x)}$ is an R-algebra isomorphism.

(IV) For any $z \in R_{q(x)}$ set $D_{q(x)}(z) := |M_{q(x)}(z)|$. Then, for any $z, z' \in R_{q(x)}$,

$$D_{q(x)}(zz') = D_{q(x)}(z)D_{q(x)}(z').$$

When $\bar{x} = (x_0, \ldots, x_{n_1}) \in R$, denote $D_{q(x)}(\bar{x}) := D_{q(x)}(z)$ where $z = \sum_{i=0}^{n-1} x_i u^i \in R_{q(x)}$.

(V) If $A \in \mathbb{M}_{q(x)}(R)$ then $\mathrm{adj}(A) \in \mathbb{M}_{q(x)}(R)$.

Using this theory, we obtain the following results (with similar proofs as in Section 5).

Theorem 6.2. *Let p be a prime, $q(x) \in \mathbb{Z}[x]$ a monic polynomial of degree $n > 0$, and let $q_0(x) \in \mathbb{F}_p[x]$ be the polynomial resulting from $q(x)$ by changing its coefficients by their residues modulo p. Then:*

(1) $q_0(x)$ is irreducible in $\mathbb{F}_p[x]$ iff the equation $D_{q(x)}(x_0, \ldots, x_{n-1}) \equiv 0 \pmod p$ does not have a non-trivial solution in the integers.

(2) If $q(x)$ is reducible in $\mathbb{Q}[x]$ then the equation $D_{q(x)}(\bar{x}) = 0$ has a non-trivial solution in the integers.

(3) If $n \geq 2$ and the equation $q_0(x) \equiv 0 \pmod{p}$ has a solution then the equation $D_{q(x)}(x_0, \ldots, x_{n-1}) \equiv 0 \pmod{p}$ has a non-trivial solution in the integers with $-p^{\frac{1}{n}} < x_i < p^{\frac{1}{n}}$ for any i.

(4) If $n \geq 2$ and $q_0(x)$ is irreducible in $\mathbb{F}_p[x]$ then the equation $D_{q(x)}(\bar{x}) = p$ does not have a solution in the integers.

As a digression, the equation $D_3^2(x_0, x_1, x_2) = p$ motivates the following.

Problem 6.3. *Assume that $a, b, c \in \{1, 2, 3\}$ and that p is a prime. Does the equation $x^a + 2y^b + 4z^c = p$ have a solution in the integers?*

(a, b, c)	Primes p where a solution was not found with `FindInstance` among the first 1000 primes
$(2, 3, 3)$	2069, 5303, 6101
$(3, 2, 3)$	2207, 2383
$(3, 3, 2)$	2039, 2083, 3371, 4027, 6143, 6997, 7699
$(3, 3, 3)$	4079, 4091, 6449, 7507

Table 1. Instances among the first 1000 primes where a solution of $x^a + 2y^b + 4z^c = p$ was not found in Wolfram Mathematica with the command `FindInstance`, in the case when at least two of a, b, c are equal to 3.

(a, b, c)	First four primes p where a solution was not found with `FindInstance`
$(2, 2, 3)$	22691, 25903, 27191, 27241
$(2, 3, 2)$	37571, 39191, 41263, 44357
$(3, 2, 2)$	24907, 51043, 51637, 53717

Table 2. First four prime p instances where a solution of $x^a + 2y^b + 4z^c = p$ was not found in Wolfram Mathematica with the command `FindInstance`, in the case when only one of a, b, c is equal to 3.

For any $p \in \mathbb{Z}$ (not necessarily prime): it is easy to find a solution when either a, b or c is equal to 1; and the case $a = b = c = 2$ has a positive answer, as mentioned in [1, §13.3, Prob. 8(a)].

So this leaves the case $2 \leq \min\{a, b, c\} \leq \max\{a, b, c\} = 3$. By running computations in Wolfram Mathematica with the command `FindInstance` (see below), a solution was not found for some primes in all the subcases (but this is not a proof that the solution does not exist).

```
FindInstance[x^a+2y^b+4z^c==p,{x,y,z},Integers]
```

See details in Tables 1 and 2: in Table 1 we look at the case when at least two of a, b, c are equal to 3, where solutions were not found for some primes below 10000; in Table 2 we look at the case when only one of a, b, c is equal to 3, where solutions were not found for some primes beyond 20000.

Acknowledgements

This work was supported by: Future Scientists School at Shizuoka University, Global Science Campus supported by the Japan Science and Technology Agency (both authors); Grant-in-Aid for Early Career Scientists 18K13448, Japan Society for the Promotion of Science (second author).

We would like to thank the anonymous referee for carefully reading the paper and for pointing out mistakes and unclear parts, which helped to improve the presentation.

References

[1] Burton D.M., *Elementary Number Theory*, McGraw Hill Education (India) Pvt Ltd, 7th Indian ed., New Delhi, 2012.

[2] Hardy G.H. and Wright E.M., *An introduction to the theory of numbers*, Oxford University Press, 6th ed., Oxford, 2008.

[3] Ireland K. and Rosen M., *A classical introduction to modern number theory from series Graduate Texts in Mathematics*, Springer-Verlag, 2nd ed., vol. 84, New York, 1990. doi: 10.1007/978-1-4757-2103-4

[4] Lang S., *Algebra from series Graduate Texts in Mathematics*, Springer-Verlag, 3rd ed., vol. 211, New York, 2002. doi: 10.1007/978-1-4613-0041-0

[5] Nathanson M.B., *Elementary Methods in Number Theory from Graduate Texts in Mathematics*, Springer-Verlag, 1st ed., vol. 195, New York, 2000. doi: 10.1007/b98870

[6] Pomerance C., "The multiplicative order mod n, on average", Quebec/Maine number theory conference at Laval University, https://math.dartmouth.edu/∼carlp/ordertalk.pdf, [cited on 18 march, 2021].

[7] Silverman J.H., "Wieferich's criterion and the *abc*-conjecture", *J. Number Theory*, 30 (1988), No. 2, 226-237. doi: 10.1016/0022-314X(88)90019-4

[8] Takagi T., *Elementary Number Theory Lectures*, Kyoritsu Shuppan, 2nd ed., Tokyo, 1971.

[9] "What is known about primes of the form $x^2 - 2y^2$?", MathOverflow. https://mathoverflow.net/questions/197918/what-is-known-about-primes-of-the-form-x2-2y2 [cited on 18 march, 2021].

[10] "What about $\mathbb{Z}[\sqrt[n]{2}]$?", Mathematics StackExchange. https://math.stackexchange.com/questions/4057721/what-about-mathbbz-sqrtn2 [cited on 18 march, 2021].