Deriving Burgess's Bound on the Distribution of Quadratic and Higher Non-Residues

Sabreen Syed
Department of Computer Science and Engineering
Indian Institute of Technology Kanpur, India

July 2018

Chapter 1

Introduction

1.1 Symbols and conventions

1.2 Preliminaries

1.3 Interval sums of quadratic residues

Chapter 2

Qualitative Analysis

In this chapter, we present a straightforward proof of a weak version of the original result discussed by Burgess in [1]. We prove the following theorem:

Theorem 1. *Given a quadratic character χ_2 modulo prime p, for any $x \in \mathbb{F}_p$ and $H > p^{1/4+\delta}$, where $\delta > 0$:*

$$\sum_{n=x+1}^{n+H} |\chi_2(n)| < H$$

for large enough p.

The starting point for our analysis is lemma 1 derived from Weil's theorem:

Lemma 1. *[1]Let $f(x)$ be a monic square-free polynomial, with coefficients from $\mathbb{Z}$, reducible into linear factors with degree ν. Then,*

$$\Big|\sum_{x=0}^{p-1} \chi_2(f(x))\Big| \leqslant (\nu - 1)p^{1/2}$$

Lemma 1 exhibits the low correlation between the distribution of values a square-free polynomial takes in $\mathbb{F}_p$ and the distribution of quadratic residues as follows: The sum of χ_2 values in an interval determines the relative count of quadratic residues and non-residues in it. The sum would cancel out to small magnitudes if the counts were nearly equal, or be closer in magnitude to the size of the interval if not. Thus, lemma 1 essentially tells us that a square free polynomial over $\mathbb{F}_p$ would assume roughly equal number of quadratic residues and non-residues over $\mathbb{F}_p$.

We deduce lemma 2 in the next section by constructing an appropriate polynomial exploiting lemma 1 for our purpose of finding low bounds on the number of continuous quadratic residues or continuous non-residues.

2.1 A useful global sum and the $O(p^{1/2})$ bound

Let us consider the sum of χ_2 values in an interval of size h.

$$S_h(x) = \sum_{n=1}^{h} \chi_2(x+n)$$

Given Lemma 1, which limits the sum of χ_2 values of a polynomial over the entire interval 0 to $p-1$, we would like to construct a square-free polynomial on which lemma 1 could be applied to successfully put a bound on the sum of χ_2 values in a smaller interval. We do this by expanding the sum $\sum_{x=0}^{p-1}(S_h(x))^{2r}$:

$$(S_h(x))^{2r} = \left(\sum_{n=1}^{h} \chi_2(x+n)\right)^{2r} = \sum_{m_1=1}^{h}\sum_{m_2=1}^{h}...\sum_{m_{2r}=1}^{h}\chi_2(x+m_1)\chi_2(x+m_2)...\chi_2(x+m_{2r})$$

$$\sum_{x=0}^{p-1}(S_h(x))^{2r} = \sum_{x=0}^{p-1}\sum_{m_1=1}^{h}\sum_{m_2=1}^{h}...\sum_{m_{2r}=1}^{h}\chi_2(x+m_1)\chi_2(x+m_2)..\chi_2(x+m_{2r})$$

$$\sum_{x=0}^{p-1}(S_h(x))^{2r} = \sum_{m_1=1}^{h}\sum_{m_2=1}^{h}...\sum_{m_{2r}=1}^{h}\sum_{x=0}^{p-1}\chi_2\big((x+m_1)(x+m_2)..(x+m_{2r})\big) \quad (2.1)$$

To use lemma 1 to estimate the expression in equation 2.1, we need to separate the perfect square polynomials forming the sum from the rest. To achieve this, we separate the ordered sequences or 'tuples' in (2.1), $(m_1, m_2...m_{2r})$, into two sets based on the multiplicity of distinct values in the tuple:

- Set 1 consists of those tuples which contain an even count of each distinct number in them. This set forms a bijective correspondence with every perfect square polynomial contributing. Since there are $\frac{(2r)!}{r!}$ ways to choose pairs of positions in a tuple and there are h^r ways of filling them with values from 1 to h, so there are less than $(2r)^r h^r$ such polynomials. Since the maximum value contributed to the sum of χ_2 values over all p values of x from each such polynomial is at most p, the contribution to the sum is at most $(2r)^r h^r p$.

- Set 2 consists of the rest of the tuples after removing set 1, which similarly correspond bijectively to the leftover polynomials exactly. Since there are h^{2r} polynomials in all, trivially at most h^{2r} are not perfect square polynomials. These polynomials are of the form:

  $$(x+s_1)^{e_1}(x+s_2)^{o_2}...(x+s_k)^{e_k}$$

  Where $s_i, i \in 1...k$ are distinct members of the tuple corresponding to the polynomial and e_i and o_i are even or odd powers respectively of the ith term. Now, $\chi\big((x+s_1)^{e_1}(x+s_2)^{o_2}...(x+s_k)^{e_k}\big)$ evaluates the same as $\chi\big((x+$

$s_2)^{o_2}...(x+s_{k'})^{o_{k'}}\big)$ (taking all odd-powered factors) for all except at most r values of x (corresponding to the even-powered factors evaluating to 0). Thus, their contribution to the sum is not more than $h^{2r}(p^{1/2}(2r-1)+r)$.

We state lemma 2, which directly follows from what we have calculated so far.

Lemma 2. *Let* $S_h(x) = \sum_{n=1}^{h} \chi_2(x+n)$. *Then,*

$$\sum_{x=0}^{p-1} |S_h(x)|^{2r} \leqslant h^r(2r)^r p + h^{2r} r(2p^{1/2}+1) \tag{2.2}$$

The $O(p^{1/2})$ bound

We prove the $O(p^{1/2})$ bound on the longest interval of continuous quadratic residues or of quadratic non-residues, i.e., we prove the following claim:

Claim. *Given a quadratic character* χ_2 *modulo prime* p*, let* h *be the greatest integer such that:*

$$\left| \sum_{n=x+1}^{x+h} \chi_2(n) \right| = h$$

for some $x \in \mathbb{F}_p$. *Then* $h \in O(p^{1/2})$.

<u>Proof:</u> We show that if the $O(p^{1/2})$ bound is not true, then lemma 2 is contradicted for large enough p.
It is given that $|S_h(z)| = h$ for some $z \in \mathbb{F}_p$. Consider the LHS of (2.2) in that case. As $|S_h(x+k)| \geqslant |S_h(x)| - 2k$,

$$\sum_{x=0}^{p-1} |S_h(x)|^{2r} \geqslant \sum_{x=z}^{z+\lfloor h/4 \rfloor} |S_h(x)|^{2r} \geqslant h^{2r} + (h-2)^{2r} + ... + (h-2\lfloor h/4 \rfloor)^{2r} \geqslant \frac{h^{2r+1}}{2^{2r+2}} \tag{2.3}$$

Thus, by considering sliding intervals starting from the original interval, we have increased the contribution to the sum from h^{2r} of the lone interval to $O(h^{2r+1})$ of the cascade of sliding intervals. Now, from (2.2) in lemma 2 and (2.3):

$$\frac{h^{2r+1}}{2^{2r+2}} \leqslant h^r(2r)^r p + h^{2r} r(2p^{1/2}+1)$$

Now we set $r = 1$ and divide both sides by h^2. We get:

$$\frac{h}{2^4} \leqslant 2h^{-1}p + (2p^{1/2}+1) \tag{2.4}$$

Substituting $cp^{1/2}$ in place of h, we obtain the inequality

$$\frac{cp^{1/2}}{16} \leqslant 2c^{-1}p^{1/2} + 2p^{1/2} + 1 \tag{2.5}$$

Comparing the coefficients of the highest power term $p^{1/2}$ on each side, we see that there exists some constant c_o such that $c/16 > 2c^{-1} + 2$ when $c > c_o$. Hence for $c > c_o$, (2.5) does not hold for large enough p. Hence, (2.4) cannot hold if $h = c_o p^{1/2}$ for large enough p. Since the LHS of (2.4) increases with increase in h, while the RHS decreases with increase in h, (2.4) cannot hold if $h > c_o p 1/2$ for large enough p, which means $h \leqslant c_o p^{1/2}$ for large enough p, and thus $h \in O(p^{1/2})$. $\diamond$

2.2 The amplification of an interval

We saw in the previous section how cascading an interval into many sliding intervals increased its contribution to the lower bound of the sum-of-intervals used in lemma 2. We now describe an additional process to increase the aforementioned contribution: We show in the following claim how an interval can be transformed into many smaller intervals which are equivalent to the original interval in terms of the distribution of quadratic residues and non-residues in them.

Claim. *Let I be an interval in $\mathbb{F}_p$ of size $H+1$. Then multiplying each element of I by q^{-1} ($q \in \mathbb{F}_p, q < p$), results in q intervals of sizes $\lfloor (H+1)/q \rfloor$ or $\lceil (H+1)/q \rceil$ throughout $\mathbb{F}_p$, with any pair of starting elements of consecutive intervals having differences $\lfloor p/q \rfloor$ or $\lceil p/q \rceil$, such that the intervals cumulatively have either the same numbers of quadratic residues and non-residues as I, or the counts of quadratic residues and non-residues are interchanged.*

<u>Proof:</u> Let I consist of the elements $\{N, N+1, ... N+H\}$. We multiply each element in I by q^{-1} resulting in the set of elements $\{Nq^{-1}, (N+1)q^{-1} ... (N+H)q^{-1}\}$, which we can refer to as Iq^{-1}. Let us work with the resulting numbers by now considering them in $\mathbb{Z}$. A general resulting element is:

$$(N+k)q^{-1} = (N+nq+s)q^{-1} = Nq^{-1} + sq^{-1} + n \tag{2.6}$$

where $k = nq + s$ and $0 \leqslant s < q$, where $n, s \in \mathbb{Z}$, by the quotient-remainder theorem. n takes values from 0 to $\lfloor (H-s)/q \rfloor$ for a particular s, since k varies from 0 to H.

We elucidate the q constructed intervals as follows: To each $Nq^{-1} + sq^{-1}$, adding a value of n from $\{0, 1, ... \lfloor (H-s)/q \rfloor\}$ results in each element of Iq^{-1} by (2.6), thus there are q small intervals of size $\lfloor (H-s)/q \rfloor$ starting at $Nq^{-1} + sq^{-1}$ for each value of s. These intervals are disjoint because, being in a field, distinct $(N+k)$ result in different values of $(N+k)q^{-1}$.

We arithmetically calculate the exact values of a small interval $\{(N+s)q^{-1}, (N+s)q^{-1} + 1, ..., (N+s)q^{-1} + \lfloor (H-s)/q \rfloor\}$. Since $N + s \equiv N + s + up \pmod p, \forall u \in \mathbb{Z}$

$$\chi((N+s)q^{-1}) = \chi((N+s+up)q^{-1})$$

For $t_1, t_2 \in \{0, 1, ...q-1\}$

$$N + s + t_1 p \equiv N + s + t_2 p \pmod{q}$$

$$\Rightarrow t_1 = t_2$$

Thus, for exactly one $t \in \{0, 1, ...q-1\}$ for each s, $N + s + tp \equiv 0 \pmod{q}$, i.e. $q \mid N + s + tp$. Now,

$$((N+s)q^{-1})q \equiv N + s \equiv N + s + tp \pmod{p}$$

$$\Rightarrow (N+s)q^{-1} \equiv \frac{N+s+tp}{q} \pmod{p}$$

since $q \mid N + s + tp$ and $\gcd(q, p) = 1$. Thus,

$$\Rightarrow (N+s)q^{-1} + m \equiv \frac{N+s+tp}{q} + m \pmod{p}$$

Hence, the small interval from $Nq^{-1} + sq^{-1}$ to $Nq^{-1} + sq^{-1} + \lfloor {}^{(H-s)}/_{q} \rfloor$ is equivalent modulo p to the integers occurring in $\left[{}^{(N+s+tp)}/_{q}, {}^{(N+s+tp+H-s)}/_{q}\right]$ which are the same as those in $\left[{}^{(N+tp)}/_{q}, {}^{(N+tp+H)}/_{q}\right]$. Since for $s_1, s_2 \in \{0, 1, ...q-1\}$,

$$N + s_1 + tp \equiv N + s_2 + tp \pmod{q}$$

$$\Rightarrow s_1 = s_2$$

Thus each value of s has a different corresponding value of t which makes $q \mid N + s + tp$. Hence, all the q intervals are equivalent modulo p to the integers between ${}^{(N+tp)}/_{q}$ and ${}^{(N+tp+H)}/_{q}$ for each $t \in \{0, 1, ...q-1\}$.

The small intervals each start at $\frac{N+s+tp}{q}$ for some s and t, thus consecutive intervals are of the form $\frac{N+s_1+tp}{q}$ and $\frac{N+s_2+(t+1)p}{q}$ since $s_i < q < p$. Thus the length between two consecutive intervals is of the form $\frac{p+\Delta s}{q}$, which can take values $\lfloor {}^{p}/_{q} \rfloor$ and $\lceil {}^{p}/_{q} \rceil$.

Multiplying the entire interval I by q^{-1} preserves or interchanges the original cardinalities of quadratic residues and non-residues in Iq^{-1}, because $\chi((N+k)q^{-1}) = \chi(q^{-1})\chi(N+k) \forall k \in \{0, 1, ..., H\}$ and $\chi(q^{-1})$ is a constant. The small intervals constructed are thus equivalent to the original interval I in this sense. $\diamond$

We now prove a lemma which allows to include many more such small intervals in a lower bound calculation of the sum-of-intervals in lemma 2 by proving that when multiplying I by several different values of q^{-1}, many of the resulting small intervals are disjoint, which will further lower the possible maximum length of any interval of only quadratic residues or only quadratic non-residues.

Lemma 3. *[1]Given are a set of Q distinct natural numbers, whose general member is given by q, which are pairwise co-prime to each other, and any natural numbers N and H such that for any q:*

$$2Hq < p \tag{2.7}$$

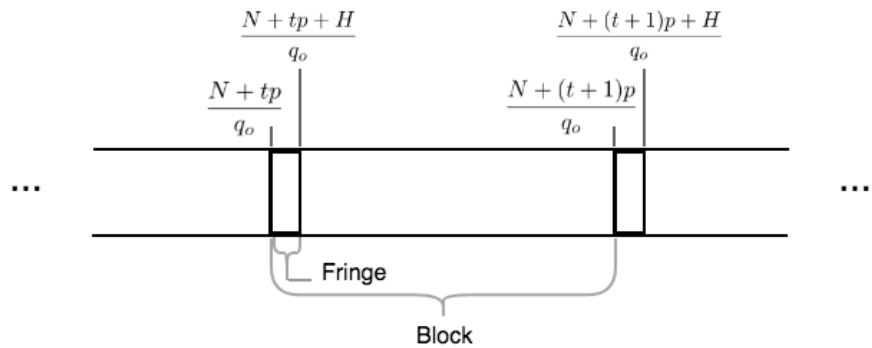

Figure 2.1: Visual representation in the number line of a block and a fringe

Let us denote by $I(q,t)$ the real interval

$$\frac{N+tp}{q} \leqslant z \leqslant \frac{N+H+tp}{q}$$

Then it is possible to associate with each q a set $T(q) \subseteq \{0,1,\ldots q-1\}$ of size at least $q-Q$, such that for each q, $\forall t \in T(q)$, $I(q,t)$ are disjoint.

Proof. For a given q, say q_o, we note that for consecutive t, $I(q_o,t)$ differ by p/q_o in their starting points. Since each $I(q_o,t)$ has a width of H/q_o and $H < p$, all $I(q_o,t)$ are disjoint for a given q_o. The $I(q_o,t)$ are in fact very narrow compared to the difference between their starting points, by a factor of $\left(\frac{H}{q_o}\right)/\left(\frac{p}{q_o}\right)$ which is less than $1/2q_o$ by (2.7). We can thus define for convenience in visualization, two terms:

- Block: The closed interval between two points on the real line, the points being the 'edges' of the block. A 'q_o-block" is the stretch between the starting points of two consecutive intervals $I(q_o,t)$ and $I(q_o,t+1)$, i.e. the closed interval with end points $(N+pt)/q_o$ and $(N+pt+p)/q_o$.

- Fringe: A narrow interval at the start of a block. A q_o-fringe is the interval $I(q_o,t)$, with respect to the block formed by the points $(N+pt)/q_o$ and $(N+pt+p)/q_o$.

They are illustrated in figure 2.1. We make the following claim about two sets of blocks:

Claim. *Let u and v be two co-prime numbers. From a point, say z, on the real line, lay blocks of length u consecutively in the positive direction of the real axis. Similarly, from z, lay blocks of size v consecutively in the positive direction as in figure 2.2. Then the first end point of blocks of size u which coincides with an end point of a block of size v, after z, are after v blocks of size u and u blocks of size v.*

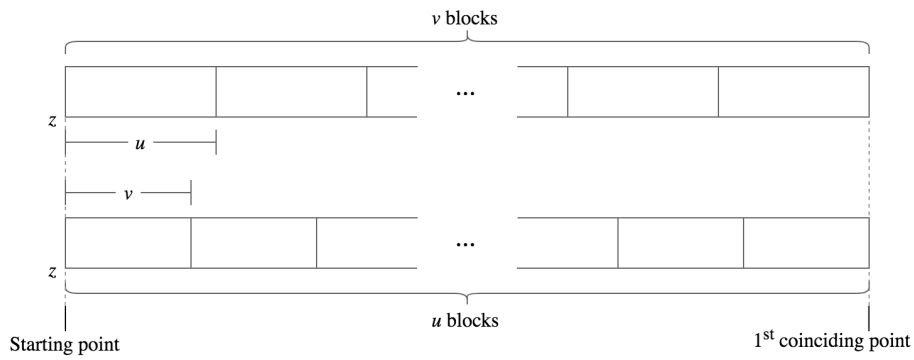

Figure 2.2: Laying blocks of co-prime sizes

<u>Proof:</u> Since, u and v are co-prime, $lcm(u, v) = uv$. If, for the sake of contradiction, say the first coinciding point was after s blocks of size u, where $s < v$, then $v \mid su \Rightarrow lcm(u, v) \leqslant su < uv$, which is a contradiction. Since $u \mid uv$ and $v \mid uv$, there is a coinciding point after v blocks of size u and u blocks of size v, which is the first coinciding point after z. $\diamond$

Now take two values of q, q_1 and q_2, and without loss of generality assume $q_1 < q_2$. The q_1-blocks are p/q_1 in size, while the q_2-blocks are of size p/q_2. If, assume, a q_1-fringe overlaps with a q_2-fringe. Then shifting the q_1-blocks by a maximum of H/q_1 in either the positive or negative direction on the real axis will align an a q_1-block edge and a q_2-block edge. Let us scale the real line by multiplying it by $q_1 q_2/p$. The resulting scaled q_1-blocks and q_2-blocks thus formed are then of lengths q_2 and q_1 respectively. Thus the points at which a q_1-block edge coincides with a q_2-block edge are separated by q_1 q_1-blocks and q_2 q_2-blocks, and also the least distance between all other pairs of edges is at least 1 in the new shifted and scaled real axis due the integer length blocks. Thus, after un-scaling the shifted real line, the point which they coincide is only after a length of p, and the length of 1 becomes $p/q_1 q_2$. So in the original unshifted and unscaled real line, a length of $p/q_1 q_2$ between a q_1-block edge and a q_2-block edge becomes a minimum of $p/q_1 q_2 - H/q_1 > H/q_1$ which is greater than both fringe widths, and hence the fringes cannot overlap in that case. Thus intervals overlap at most once in a length of p.

Thus we can eliminate at most one t from $T(q_1)$ and one t from $T(q_2)$ while considering the intersections for the pair (q_1, q_2). Hence, for each q, there are at least $q - Q$ values of $t \in \{0, 1, \ldots q - 1\}$ such that $I(q, t)$ are disjoint from all other intervals associated with all q.

$\square$

Hence, we can now see that multiplying an interval I in $\mathbb{F}_p$ by many values of q^{-1} for appropriate values of q, can lead to many non-intersecting small intervals in $\mathbb{F}_p$ which are very similar to the original interval I in terms of the number of quadratic residues and non-residues in them. These non-intersecting intervals

can be cascaded as in eq. 2.3 and summed in a lower bound calculation of the sum-of-intervals in lemma 2, to further lower the bound of $O(p^{1/2})$. This leads to the $O(p^{1/4+\delta})$ bound on the least quadratic residue, which we now proceed to prove in the next section.

2.3 The $p^{1/4+\delta}$ bound

We now proceed to proving the bound on the least quadratic non-residue, i.e. Theorem 1, using the results proven thus. We restate the theorem:

Theorem. *Given a quadratic character χ_2 modulo prime p, for any $x \in \mathbb{F}_p$ and $H > p^{1/4+\delta}$, where $\delta > 0$:*

$$\sum_{n=x+1}^{n+H} |\chi_2(n)| < H$$

for large enough p.

Proof. The proof is by means of contradiction. Let us assume there exists an $H > p^{1/4+\delta}$ such that for some $\delta > 0$, and $\left|\sum_{x=N+1}^{N+H} \chi_2(x)\right| = H$. We already know that for $H > cp^{1/2}$, where c is some constant, there can be no interval of all quadratic residues or all non-residues. Thus, $H \leqslant cp^{1/2}$.
We take numbers given by q, pair-wise co-prime (as required for the application of lemma 3 later), to be the primes in the range:

$$\frac{p^{1/4}}{2} \leqslant q \leqslant p^{1/4}$$

This satisfies the constraint in (2.7) for large enough p. The number of primes q is given by $Q = \pi(p^{1/4}) - \pi(\frac{p^{1/4}}{2}) = o(p^{1/4})$ by the prime number theorem. Now, restating the assumption:

$$\left|\sum_{x=N+1}^{N+H} \chi_2(x)\right| = H \tag{2.8}$$

In the next few steps, we proceed to transform the interval in eq. 2.8 into several smaller intervals as discussed in the previous section. For a fixed x, $x + tp$ is divisible by q for exactly one value of $t \in \{0, 1, ...q-1\}$. Also $\chi(x + tp) = \chi(x)$. Thus:

$$\left|\sum_{x=N+1}^{N+H} \chi_2(x)\right| = \left|\sum_{t=0}^{t=q-1} \sum_{\substack{x=N+1 \\ x+tp \mid q}}^{N+H} \chi_2(x + tp)\right| = H$$

Since $q \mid x + tp$, thus $x + tp = qz$ for some $z \in \mathbb{Z}$, $\Rightarrow z = \frac{x+tp}{q}$.
For $N + 1 \leqslant x \leqslant N + H$, we see that all such corresponding z obtained are the

integer values in $I(q,t)$ according to lemma 3, t being the corresponding values such that $q \mid x+tp$.

$$\Big|\sum_{t=0}^{t=q-1}\sum_{\substack{x=N+1\\ q\,|\,x+tp}}^{N+H}\chi_2\Big(\frac{x+tp}{q}.q\Big)\Big| = H$$

$$\Big|\sum_{t=0}^{t=q-1}\sum_{z\in I(q,t)}\chi_2(z.q)\Big| = H$$

$$\Big|\sum_{t=0}^{t=q-1}\sum_{z\in I(q,t)}\chi_2(z)\chi_2(q)\Big| = H$$

Now, since $|a|+|b| \geqslant |a+b|$

$$\sum_{t=0}^{t=q-1}\Big|\sum_{z\in I(q,t)}\chi_2(z)\chi_2(q)\Big| \geqslant H$$

$$\sum_{q}\sum_{t=0}^{t=q-1}\Big|\chi_2(q)\sum_{z\in I(q,t)}\chi_2(z)\Big| \geqslant HQ$$

$$\sum_{q}\Big|\chi_2(q)\Big|\sum_{t=0}^{t=q-1}\Big|\sum_{z\in I(q,t)}\chi_2(z)\Big| \geqslant HQ$$

$$\sum_{q}\sum_{t=0}^{t=q-1}\Big|\sum_{z\in I(q,t)}\chi_2(z)\Big| \geqslant HQ$$

Separating the possibly overlapping intervals from the disjoint intervals:

$$\sum_{q}\sum_{t\in T(q)}\Big|\sum_{z\in I(q,t)}\chi_2(z)\Big| + \sum_{q}\sum_{\substack{t=0\\ t\notin T(q)}}^{q-1}\Big|\sum_{z\in I(q,t)}\chi_2(z)\Big| \geqslant HQ \tag{2.9}$$

Now,

$$\sum_{q}\sum_{\substack{t=0\\ t\notin T(q)}}^{q-1}\Big|\sum_{z\in I(q,t)}\chi_2(z)\Big| \leqslant \sum_{q} Q\left\lceil\frac{H}{q}\right\rceil \leqslant \sum_{q} Q\frac{2H}{q} < 4Q^2Hp^{-1/4} \tag{2.10}$$

since $\sum_{q} q^{-1} < Q.\Big(\frac{p^{1/4}}{2}\Big)^{-1}$. Using 2.9 and 2.10,

$$\sum_{q}\sum_{t\in T(q)}\Big|\sum_{z\in I(q,t)}\chi_2(z)\Big| > HQ - 4Q^2Hp^{1/4} = HQ(1-4Qp^{-1/4}) > \frac{HQ}{2} \tag{2.11}$$

for large enough p, since $Q = o(p^{1/4})$. Since all $I(q,t)$ such that $t \in T(q)$ are mutually disjoint, and $\bigcup_q \bigcup_{t \in T(q)} I(q,t) \subseteq \{0,1,...,p-1\}$, $\sum_q \sum_{t \in T(q)} \sum_{z \in I(q,t)} |S_h| \leqslant \sum_{x=0}^{p-1} |S_h(x)|^{2r}$ according to lemma 2. Thus, converting the left-most side of eq. 2.11 in a compatible form with lemma 2 can help put an upper bound on it, which we now aim to do.

$$\sum_{z \in I(q,t)} \chi_2(z+m) = \sum_{z \in I(q,t)} \chi_2(z) - \phi_m$$

where $\phi_m \leqslant 2m$

$$\sum_{m=0}^{h-1} \sum_{z \in I(q,t)} \chi_2(z+m) = \sum_{m=0}^{h-1} \sum_{z \in I(q,t)} \chi_2(z) - \sum_{m=0}^{h-1} \phi_m$$

$$\sum_{m=0}^{h-1} \sum_{z \in I(q,t)} \chi_2(z+m) + \sum_{m=0}^{h-1} \phi_m = h \sum_{z \in I(q,t)} \chi_2(z)$$

$$\left| \sum_{m=0}^{h-1} \sum_{z \in I(q,t)} \chi_2(z+m) + \sum_{m=0}^{h-1} \phi_m \right| = \left| h \sum_{z \in I(q,t)} \chi_2(z) \right|$$

Since $|a| + |b| \geqslant |a+b|$,

$$\sum_{z \in I(q,t)} \left| \sum_{m=0}^{h-1} \chi_2(z+m) \right| + \left| \sum_{m=0}^{h-1} \phi_m \right| \geqslant h \left| \sum_{z \in I(q,t)} \chi_2(z) \right|$$

$$\sum_{z \in I(q,t)} \left| \sum_{m=0}^{h-1} \chi_2(z+m) \right| \geqslant h \left| \sum_{z \in I(q,t)} \chi_2(z) \right| - h^2$$

$$\sum_q \sum_{t \in T(q)} \sum_{z \in I(q,t)} \left| \sum_{m=0}^{h-1} \chi_2(z+m) \right| \geqslant h \sum_q \sum_{t \in T(q)} \left| \sum_{z \in I(q,t)} \chi_2(z) \right| - Qp^{1/4}h^2 \quad (2.12)$$

since the number of the disjoint intervals $I(q,t)$ given by lemma 3 are less than $Qp^{1/4}$. To estimate the RHS from eq. 2.11:

$$\sum_{m=0}^{h-1} \sum_q \sum_{t \in T(q)} \left| \sum_{z \in I(q,t)} \chi_2(z) \right| = h \sum_q \sum_{t \in T(q)} \left| \sum_{z \in I(q,t)} \chi_2(z) \right| > \frac{HhQ}{2} \quad (2.13)$$

So from (2.13) and (2.12)

$$\sum_q \sum_{t \in T(q)} \sum_{z \in I(q,t)} \left| \sum_{m=0}^{h-1} \chi_2(z+m) \right| > \frac{HhQ}{2} - Qp^{1/4}h^2 = Qh\big(\frac{H}{2} - hp^{1/4}\big)$$

Taking $h < \frac{1}{4}p^{-1/4}H$, and using the the definition of S_h from lemma 2,

$$\sum_q \sum_{t\in T(q)} \sum_{z\in I(q,t)} |S_h(z)| > \frac{HhQ}{4}$$

Using Holder's inequality,

$$\sum_q \sum_{t\in T(q)} \sum_{z\in I(q,t)} |S_h(z)| \leqslant \left(\sum_q \sum_{t\in T(q)} \sum_{z\in I(q,t)} |S_h(z)|^{2r}\right)^{1/2r} \left(\sum_q \sum_{t\in T(q)} \sum_{z\in I(q,t)} 1\right)^{1-1/2r}$$

$$\sum_q \sum_{t\in T(q)} \sum_{z\in I(q,t)} |S_h(z)|^{2r} \geqslant \left(\sum_q \sum_{t\in T(q)} \sum_{z\in I(q,t)} |S_h(z)|\right)^{2r} \left(\sum_q \sum_{t\in T(q)} \sum_{z\in I(q,t)} 1\right)^{-(2r-1)}$$

$$\sum_q \sum_{t\in T(q)} \sum_{z\in I(q,t)} |S_h(z)|^{2r} > \left(\frac{HhQ}{4}\right)^{2r} \left(Qp^{1/4}.2.\frac{H}{p^{1/4}}\right)^{-(2r-1)}$$

$$\sum_{z=0}^{p-1} |S_h(z)|^{2r} > \left(\frac{1}{8}\right)^{2r} HQh^{2r}$$

From lemma 2,

$$(2r)^r h^r p + h^{2r} r(2p^{1/2}+1) > \left(\frac{1}{8}\right)^{2r} HQh^{2r}$$

For large enough p, the second term of the LHS diminishes compared to the RHS, because:

$$\frac{h^{2r} r(2p^{1/2}+1)}{\left(\frac{1}{8}\right)^{2r} HQh^{2r}} \leqslant c\frac{p^{1/2}}{HQ} \leqslant c\frac{\log p}{p^{\delta}} < 1$$

where c is a placeholder for any constant, since $HQ \geqslant \frac{p^{1/2+\delta}}{4\log p}$. Now, we take $h = \left\lfloor \frac{1}{5}p^{-1/4}H \right\rfloor$. Taking some value of $r > \delta^{-1}$ results in the first term of the LHS diminishing with respect to the RHS, as:

$$\frac{(2r)^r h^r p}{\left(\frac{1}{8}\right)^{2r} HQh^{2r}} \leqslant c\frac{p\log p}{p^{1/2+\delta}h^r} < c\frac{p^{1/2}\log p}{p^{\delta}.p} \leqslant c\frac{\log p}{p^{1/2+\delta}} < 1$$

since $h > (1/6)p^{\delta}$, for large enough p. Thus, we have arrived at a contradiction. Our assumption that $\left|\sum_{x=N+1}^{N+H} \chi_2(x)\right| = H$ for $H > p^{1/4+\delta}$ for large enough p was wrong. Hence, the only possibility is that $\left|\sum_{x=N+1}^{N+H} \chi_2(x)\right| < H$ for $H > p^{1/4+\delta}$ for large enough p, for any $\delta > 0$, proving Theorem 1. $\square$

2.4 Extension to general characters

Now we consider a natural extension of what we have proven so far: extending the result to general characters, i.e. finding an upper bound on the largest interval of elements in which a character assumes the same value. Formally,

Theorem 2. *Given a character χ modulo prime p, for any $x \in \mathbb{F}_p$ and $H > p^{1/4+\delta}$, where $\delta > 0$:*

$$\sum_{n=x+1}^{n+H} |\chi(n)| < H$$

for large enough p.

Although a more general form of lemma 1 for general characters exists, a possible impediment in reapplying the former proof technique is dealing with the complex numbers involved in general characters. But as it turns out, we can easily extend the previously used techniques and theorems in the complex domain to obtain the same results for a general character.

The general form of lemma 1 for any character is:

Lemma 4. *[6]Let χ be a non-trivial character of order d. Let $f(x)$ be a polynomial which is not a perfect d^{th} power, with coefficients from $\mathbb{Z}$. Let $f(x)$ have ν distinct zeroes. Then,*

$$\Big|\sum_{x=0}^{p-1} \chi(f(x))\Big| \leqslant (\nu - 1)p^{1/2}$$

We henceforth assume $d \mid p-1$, because since $\chi^d(x) = 1$ and $\chi(x^{p-1}) = \chi^{p-1}(x) = 1$ for $x \neq 0$, $\chi^{gcd(d,p-1)}(x) = 1$ for $x \neq 0$, and hence any character of order d is also a character of order $gcd(d, p-1)$ using Euclid's algorithm, and hence we consider $gcd(d, p-1)$ as the character order. We now use lemma 4 to derive lemma 2 for a general character.

2.4.1 Proving Lemma 2 for a General Character

We define

$$S_h(x) = \sum_{n=0}^{h-1} \chi(x+n) \tag{2.14}$$

We then expand the sum $|S_h(x)|^{2r}$:

$$|S_h(x)|^{2r} = \Big|\sum_{n=0}^{h-1} \chi(x+n)\Big|^{2r} = \Big(\sum_{n=0}^{h-1} \chi(x+n)\Big)^r \overline{\Big(\sum_{n=0}^{h-1} \chi(x+n)\Big)}^r$$

$$|S_h(x)|^{2r} = \Big(\sum_{m_1=1}^{h}\sum_{m_2=1}^{h}...\sum_{m_r=1}^{h}\chi(x+m_1)\chi(x+m_2)...\chi(x+m_r)\Big)$$
$$\Big(\sum_{m_{r+1}=1}^{h}\sum_{m_{r+2}=1}^{h}...\sum_{m_{2r}=1}^{h}\overline{\chi(x+m_{r+1})\chi(x+m_{r+2})...\chi(x+m_{2r})}\Big)$$

$$|S_h(x)|^{2r} = \Big(\sum_{m_1=1}^{h}\sum_{m_2=1}^{h}...\sum_{m_r=1}^{h}\chi\big((x+m_1)(x+m_2)...(x+m_r)\big)\Big)$$
$$\Big(\sum_{m_{r+1}=1}^{h}\sum_{m_{r+2}=1}^{h}...\sum_{m_{2r}=1}^{h}\overline{\chi}\big((x+m_{r+1})(x+m_{r+2})...(x+m_{2r})\big)\Big)$$

Using the property of a character that $\overline{\chi}(x) = \chi(x^{-1})$ for $x \neq 0$:

$$|S_h(x)|^{2r} = \Big(\sum_{m_1=1}^{h}\sum_{m_2=1}^{h}...\sum_{m_r=1}^{h}\chi\big((x+m_1)(x+m_2)...(x+m_r)\big)\Big)$$
$$\Big(\sum_{m_{r+1}=1}^{h}\sum_{m_{r+2}=1}^{h}...\sum_{m_{2r}=1}^{h}\chi\big((x+m_{r+1})^{p-2}(x+m_{r+2})^{p-2}...(x+m_{2r})^{p-2}\big)\Big)$$
$$= \sum_{m_1=1}^{h}\sum_{m_2=1}^{h}...\sum_{m_{2r}=1}^{h}\chi\big((x+m_1)(x+m_2)...(x+m_r)\big((x+m_{r+1})(x+m_{r+2})...(x+m_{2r})\big)^{p-2}\big)$$
$$\sum_{x=0}^{p-1}|S_h(x)|^{2r} = \sum_{m_1=1}^{h}\sum_{m_2=1}^{h}...\sum_{m_{2r}=1}^{h}\sum_{x=0}^{p-1}\chi\Big(\prod_{i=1}^{r}(x+m_i)\prod_{i=r+1}^{2r}(x+m_i)^{p-2}\Big) \quad (2.15)$$

In equation 2.15, we must separate the perfect d^{th} power polynomials formed in the sum from the rest. We do this, again as in the case of quadratic character, by examining the tuples formed by $(m_1, m_2...m_{2r})$:

- **Perfect d^{th} power polynomials:** Since $d \mid p-1 \Rightarrow \gcd(d, p-2) = 1$, no power of $(x+m)^{p-2}$ less than the dth power will form a perfect d^{th} power polynomial. Thus, a tuple represents a perfect d^{th} power polynomial if the occurrence of each element in $\{m_1, m_2...m_r\}$ can be paired bijectively with an occurrence of the same element in $\{m_{r+1}, m_{r+2}...m_{2r}\}$, and the rest of the occurrences of elements in $m_1, m_2, ..., m_r$ are in a multiple of d, and the rest of the occurrences of elements in $m_{r+1}, m_{r+2}...m_{2r}$ are also in a multiple of d. Thus the total number of such polynomials is:

$$\sum_{k=1}^{\lfloor r/d\rfloor}\left(\frac{\binom{r}{d}\binom{r-d}{d}...\binom{r-(k-1)d}{d}}{k!}\right)^2\frac{\binom{r-kd}{1}^2\binom{r-kd-1}{1}^2...\binom{1}{1}^2}{(r-kd)!}h^{2k+r-kd}$$
$$\leqslant (r!)^2h^r\sum_{k=1}^{\lfloor r/d\rfloor}\max_k\frac{1}{(d!)^{2k}(r-kd)!(k!)^2} \leqslant \frac{r}{d}.(r!)^2h^r \leqslant r^{2r}h^r$$

  Thus, these polynomials contribute at most $r^{2r}h^rp$ to the sum in 2.15.

- **The remaining polynomials:** The total no. of the rest of the polynomials is trivially at most h^{2r}. Thus, these contribute at most $h^{2r}(2r-1)p^{1/2}$.

Hence, we arrive at the following lemma, which is a general version of lemma 2:

Lemma. *Let* $S_h(x) = \sum_{n=1}^{h} \chi(x+n)$. *Then,*

$$\sum_{x=0}^{p-1} |S_h(x)|^{2r} \leqslant h^r(2r)^r p + 2h^{2r} r p^{1/2} \leqslant h^r(2r)^r p + h^{2r} r(2p^{1/2}+1) \tag{2.16}$$

We will refer to this lemma as lemma 2, and it being for a general character can be inferred from the context of usage.

Now, we can derive the $O(p^{1/2})$ and $p^{1/4+\delta}$ bounds for general characters using almost identical methods as those for quadratic residues. We derive both the $O(p^{1/2})$ bound and the $p^{1/4+\delta}$ bound by mimicking most steps with minor changes in assumptions and reasoning. We also eliminate many steps and accompanying explanations, for brevity and reducing repetitiveness.

2.4.2 The $O(p^{1/2})$ bound for a general character

We prove the bound of $O(p^{1/2})$ on the largest interval of elements in $\mathbb{F}_p$ on which χ assumes the same value. Formally:

Claim. *Given a character* χ_2 *modulo prime* p*, let* h *be the greatest integer such that:*

$$\left| \sum_{n=x+1}^{x+h} \chi(n) \right| = h$$

for some $x \in \mathbb{F}_p$. *Then* $h \in O(p^{1/2})$.

<u>Proof:</u> We arrive at the result by contradiction as in the case of quadratic characters. Let the largest interval of elements in $\mathbb{F}_p$, on which χ assumes the same value, be given by h. Then, using the definition in equation 2.14, $|S_h(z)| = h$. Then we can say,

$$\sum_{x=0}^{p-1} |S_h(x)|^{2r} \geqslant \sum_{x=z}^{z+\lfloor h/4 \rfloor} |S_h(x)|^{2r} \geqslant h^{2r} + (h-2)^{2r} + ... + (h - 2\lfloor h/4 \rfloor)^{2r} \geqslant \frac{h^{2r+1}}{2^{2r+2}} \tag{2.17}$$

as $|S_h(x+k)| \geqslant |S_h(x)| - 2k$. Then from equations 2.16 and 2.17:

$$\frac{h^{2r+1}}{2^{2r+2}} \leqslant h^r(2r)^r p + h^{2r} r(2p^{1/2}+1)$$

Take $r = 1$ and divide both sides by h^2. We get:

$$\frac{h}{2^4} \leqslant 2h^{-1}p + (2p^{1/2}+1) \tag{2.18}$$

Substituting $cp^{1/2}$ in place of h, we obtain the inequality

$$\frac{cp^{1/2}}{16} \leqslant 2c^{-1}p^{1/2} + 2p^{1/2} + 1 \tag{2.19}$$

Comparing the coefficients of the highest power term $p^{1/2}$ on each side, we see that there exists some constant c_o such that $c/16 > 2c^{-1} + 2$ when $c > c_o$. Hence for $c > c_o$, (2.18) does not hold for large enough p. Hence, (2.19) cannot hold if $h = c_o p^{1/2}$ for large enough p. Since the LHS of (2.18) increases with increase in h, while the RHS decreases with increase in h, (2.18) cannot hold if $h > c_o p1/2$ for large enough p, which means $h \leqslant c_o p^{1/2}$ for large enough p, and thus $h \in O(p^{1/2})$. ◇

2.4.3 The $p^{1/4+\delta}$ bound for a general character

We prove the upper bound of $p^{1/4+\delta}$, where $\delta > 0$, on the largest interval of elements in $\mathbb{F}_p$ on which χ assumes the same value, i.e. Theorem 2. We restate the theorem:

Theorem. *Given a character χ modulo prime p, for any $x \in \mathbb{F}_p$ and $H > p^{1/4+\delta}$, where $\delta > 0$:*

$$\sum_{n=x+1}^{n+H} |\chi(n)| < H$$

for large enough p.

Proof. We prove the theorem by contradiction. Say for some $H > p^{1/4+\delta}$, for some $\delta > 0$, $\left|\sum_{x=N+1}^{N+H} \chi(x)\right| = H$ for large enough p. We know that for $H > cp^{1/2}$, where c is some appropriate constant, there can be no interval where χ assumes the same value. Thus, $H \leqslant cp^{1/2}$
We take numbers given by q, pair-wise co-prime (as required for the application of lemma 3 later), to be the primes in the range:

$$\frac{p^{1/4}}{2} \leqslant q \leqslant p^{1/4}$$

This satisfies the constraint in (2.7) for large enough p. The number of primes q is given by $Q = \pi(p^{1/4}) - \pi(\frac{p^{1/4}}{2}) = o(p^{1/4})$ by the prime number theorem. Now proceeding with the proof:

$$\left|\sum_{x=N+1}^{N+H} \chi(x)\right| = \left|\sum_{t=0}^{t=q-1} \sum_{\substack{x=N+1 \\ x+tp \mid q}}^{N+H} \chi(x+tp)\right| = H$$

$$\left|\sum_{t=0}^{t=q-1} \sum_{\substack{x=N+1 \\ x+tp \mid q}}^{N+H} \chi\Big(\frac{x+tp}{q}.q\Big)\right| = H$$

$$\Big|\sum_{t=0}^{t=q-1}\sum_{z\in I(q,t)}\chi(z)\chi(q)\Big| = H$$

$$\sum_{t=0}^{t=q-1}\Big|\sum_{z\in I(q,t)}\chi(z)\chi(q)\Big| \geqslant H$$

$$\sum_{q}\sum_{t=0}^{t=q-1}\Big|\sum_{z\in I(q,t)}\chi(z)\Big| \geqslant HQ$$

$$\sum_{q}\sum_{t\in T(q)}\Big|\sum_{z\in I(q,t)}\chi(z)\Big| + \sum_{q}\sum_{\substack{t=0\\ t\notin T(q)}}^{q-1}\Big|\sum_{z\in I(q,t)}\chi(z)\Big| \geqslant HQ \tag{2.20}$$

Now,

$$\sum_{q}\sum_{\substack{t=0\\ t\notin T(q)}}^{q-1}\Big|\sum_{z\in I(q,t)}\chi(z)\Big| < 4Q^2Hp^{-1/4} \tag{2.21}$$

Using 2.20 and 2.21,

$$\sum_{q}\sum_{t\in T(q)}\Big|\sum_{z\in I(q,t)}\chi(z)\Big| > \frac{HQ}{2}$$

$$\sum_{m=0}^{h-1}\sum_{q}\sum_{t\in T(q)}\Big|\sum_{z\in I(q,t)}\chi(z)\Big| > \frac{HhQ}{2} \tag{2.22}$$

for large enough p. Now, we have

$$\sum_{z\in I(q,t)}\chi(z+m) = \sum_{z\in I(q,t)}\chi(z) + \sum_{i=1}^{m}\chi(b_i) - \sum_{i=1}^{m}\chi(d_i)$$

where $b_i, d_i \in \mathbb{F}_p$. This implies

$$\sum_{m=0}^{h-1}\sum_{z\in I(q,t)}\chi(z+m) = \sum_{m=0}^{h-1}\sum_{z\in I(q,t)}\chi(z) + \sum_{m=0}^{h-1}\Big(\sum_{i=1}^{m}\chi(b_i) - \sum_{i=1}^{m}\chi(d_i)\Big)$$

$$\Big|\sum_{m=0}^{h-1}\sum_{z\in I(q,t)}\chi(z+m)\Big| = \Big|\sum_{m=0}^{h-1}\sum_{z\in I(q,t)}\chi(z) + \sum_{m=0}^{h-1}\Big(\sum_{i=1}^{m}\chi(b_i) - \sum_{i=1}^{m}\chi(d_i)\Big)\Big|$$

$$\Big|\sum_{m=0}^{h-1}\sum_{z\in I(q,t)}\chi(z+m)\Big| \geqslant h\Big|\sum_{z\in I(q,t)}\chi(z)\Big| - \Big|\sum_{m=0}^{h-1}\Big(\sum_{i=1}^{m}\chi(b_i) - \sum_{i=1}^{m}\chi(d_i)\Big)\Big|$$

$$\sum_{m=0}^{h-1}\Big|\sum_{z\in I(q,t)}\chi(z+m)\Big| \geqslant h\Big|\sum_{z\in I(q,t)}\chi(z)\Big| - \Big|\sum_{m=0}^{h-1}2m\Big| \geqslant h\Big|\sum_{z\in I(q,t)}\chi(z)\Big| - h^2$$

$$\sum_q \sum_{t\in T(q)} \sum_{z\in I(q,t)} \left| \sum_{m=0}^{h-1} \chi(z+m) \right| \geqslant h \sum_q \sum_{t\in T(q)} \left| \sum_{z\in I(q,t)} \chi(z) \right| - Qp^{1/4}h^2$$

So from equation 2.4.3

$$\sum_q \sum_{t\in T(q)} \sum_{z\in I(q,t)} \left| \sum_{m=0}^{h-1} \chi(z+m) \right| > Qh\big(\frac{H}{2} - hp^{1/4}\big)$$

Taking $h < \frac{1}{4}p^{-1/4}H$, and using the terminology from 2.14,

$$\sum_q \sum_{t\in T(q)} \sum_{z\in I(q,t)} |S_h(z)| > \frac{HhQ}{4}$$

Using Holder's inequality,

$$\sum_q \sum_{t\in T(q)} \sum_{z\in I(q,t)} |S_h(z)| \leqslant \left(\sum_q \sum_{t\in T(q)} \sum_{z\in I(q,t)} |S_h(z)|^{2r} \right)^{1/2r} \left(\sum_q \sum_{t\in T(q)} \sum_{z\in I(q,t)} 1 \right)^{1-1/2r}$$

$$\sum_{z=0}^{p-1} |S_h(z)|^{2r} > \sum_q \sum_{t\in T(q)} \sum_{z\in I(q,t)} |S_h(z)|^{2r} > \left(\frac{1}{8}\right)^{2r} HQh^{2r}$$

From lemma 2,

$$(2r)^r h^r p + h^{2r} r(2p^{1/2}+1) > \left(\frac{1}{8}\right)^{2r} HQh^{2r}$$

For large enough p, the second term of the LHS diminishes compared to the RHS as $HQ \geqslant \frac{p^{1/2+\delta}}{4\log p}$. Now, we take $h = \lfloor \frac{1}{5}p^{-1/4}H \rfloor$. We take $r > \delta^{-1}$, which results in the first term of the LHS diminishing with respect to the RHS for large enough p.

Thus, we have arrived at a contradiction. Our assumption that $\left| \sum_{x=N+1}^{N+H} \chi(x) \right| = H$ for $H > p^{1/4+\delta}$ for large enough p was wrong. Hence, the only possibility is that $\left| \sum_{x=N+1}^{N+H} \chi(x) \right| < H$ for $H > p^{1/4+\delta}$ for large enough p, for any $\delta > 0$, proving Theorem 2. $\square$

Chapter 3

Extensions to quadratic functions of intervals

In this chapter, we describe a solution to a subproblem of factorizing polynomials in finite fields, the worst-case complexity of which can be bounded by extending the the scope of lemma 2. We will also look at why theorem 1 cannot be extended to improve the solution.

3.1 The problem and a solution

Factorizing polynomials in finite fields, while being an interesting problem on its own, is also a relevant problem to many areas, like coding theory and cryptography. A basic subproblem of it is factorizing a univariate quadratic polynomial in $\mathbb{F}_p$. We now formally describe this problem.

Aim. *Given a quadratic univariate polynomial $f(x) = ax^2 + bx + c$, $a \neq 0$ with $a, b, c \in \mathbb{F}_p$, determine both its (non-constant) factors $(x + d)$ and $(x + e)$ such that $f(x) = a(x + d)(x + e)$, if such factors exist.*

Since checking for square factors of quadratic polynomials can easily be done by checking if $b^2 = 2^2ac$, for the rest of the chapter we only consider the aim of factorizing square-free polynomials.

Say $f(x)$ is completely factorizable in $\mathbb{F}_p$ with factors $(x + d)$ and $(x + e)$. Since the gcd of two polynomials can be calculated in $\log d_e$ time, where d_e is the maximum of the degrees of both polynomials, so calculating the gcd of $f(x)$ and a polynomial (say represented generically by $g(x)$) with known factors can be an efficient method of testing if $f(x)$ contains any of the known factors. Thus, if we were to take some $g(x)$ having exactly one of $(x + d)$ and $(x + e)$ as a factor, say in this case the factor $(x + d)$, then

$$\gcd(f(x), g(x)) = (x + d)$$

and thus we can easily factorise $f(x)$ by dividing it by $(x+d)$ using polynomial long division. Along that line, we consider the polynomial $x^{\frac{p-1}{2}} - 1$. It is of small size ($O(1)$), while having as factors exactly half of the set $\{(x+1),(x+2),...(x+p-1)\}$, i.e. precisely those $(x+i), i \in \mathbb{F}_p$ such that i is a quadratic residue mod p because for $j \in \mathbb{F}_p$:

$$j^{\frac{p-1}{2}} = 1 \Leftrightarrow j \text{ is a quadratic residue}$$

Thus taking its gcd with any quadratic polynomial takes low memory as well as time, with an intuitively good chance of exactly one factor of the quadratic polynomial as the gcd. We now detail an initial solution to acheive our aim:

<u>Solution:</u> Let $g(x) = x^{\frac{p-1}{2}} - 1$. Compute the gcd of $f(x)$ and $g(x)$. If the result is a linear polynomial, say $(x+k)$, then $f(x)$ can easily be factorised by plynomial division. If, however, the result is not a linear polynomial, and is instead constant or quadratic, we apply a trick: We compute the gcd of $g(x)$ and $f(x+1)$. If $f(x)$ is factorisable with factors $(x+d)$ and $(x+e)$, then $f(x+1)$ has factors $(x+d+1)$ and $(x+e+1)$. The factors of $f(x+1)$ are, thus, (generally) different from the factors of $f(x)$.

Thus, despite the gcd of $g(x)$ and $f(x)$ not being linear, the gcd of $g(x)$ and $f(x+1)$ may be a linear polynomial. If it is not linear again, we reapply our trick repeatedly to increment the argument of polynomial function f by constant 1 at each application, till we obtain an $i \in \mathbb{F}_p$ such that the gcd of $g(x)$ and $f(x+i)$ is a linear polynomial. We then factorize $f(x+i)$ using its gcd with $g(x)$, to obtain the factors say $(x+d_i)$ and $(x+e_i)$ of $f(x+i)$ such that $f(x+i) = a(x+d_i)(x+e_i)$. Then $f(x) = a(x-i+d_i)(x-i+e_i)$, and thus the factors of $f(x)$ are $(x+e_i-i)$ and $(x+d_i-i)$.

However, if we are unable to obtain such an i that the gcd of $g(x)$ and $f(x+i)$ is a linear polynomial throughout $\mathbb{F}_p$, we conclude that $f(x)$ is irreducible in $\mathbb{F}_p$. $\diamond$

The worst-case time complexity of the above solution is $O(p \log p)$, which is worse than if we had simply divided $f(x)$ by each possible linear factor. However, if we we prove an upper bound on the size of i such that gcd of $g(x)$ and $f(x+i)$ is a linear polynomial if $f(x)$ is factorizable, we can drastically improve the worst-case time complexity, since if no such i is found in the solution uptil the upper bound, we can safely conclude it is irreducible.

3.2 Problems with attempts at further generalisation

Chapter 4

Quantitative Analysis

4.1 Energy

4.2 Sieving

4.3

Bibliography

[1] D. A. Burgess, *The distribution of quadratic residues and non-residues*, Mathematika 4 (1957), 106-112.

[2] David M. Burton, *Elementary Number Theory*, McGraw Hill, 2012.

[3] S. Lindhurst, *An analysis of Shanks's algorithm for computing square roots in finite fields*, CRM Proceedings and Lecture Notes, Vol. 19 (1999) pp. 231–242.

[4] G. Polya, *"Über die Verteilung der quadratischen Eeste und Nichtreste"*, Göttinger Nachrichten (1918), 21-29.

[5] I. M. Vinogradov, *"Sur la distribution des résidus et des non-résidus des puissances "*, Journal Physico-Math. Soc. Univ. Perm, No. 1 (1918), 94-96.

[6] W. Schmidt, *"Equations over finite fields, An elementary approach"*, Lecture Notes in Math. 536, Springer Verlag, 1976, p. 43