PLACES FROM A SPHERE

Prerequisites. The structure of $(\mathbb{Z}/p^c\mathbb{Z})^\times$ for a prime p [IR, Ch. 4, §1]. Linearity of expectation. From Chapter 3 we use the places Φ of E and their labels, the reduction cl of the label modulo q_0, the place $[\nu]$ of an integer ν, the a-places Φ_a and the b-places Φ_b (Section 3.1), and Problems 3.1.3, 3.1.6 and 3.3.2. From Chapter 33, the admissible data. We write $U_m := (\mathbb{Z}/m\mathbb{Z})^\times$ for $m \geq 1$.

In Chapter 3 a set Φ_b of places of class -1 modulo q_0 was given the weight b, and Problem 3.3.2 showed why it must be dense: if $b > 1$ and $\#\Phi_a \leq \#\Phi_b \log b$, then

$$R_{q_0}(x) \leq \frac{\text{rem}}{a\,\#\Phi_b} + |R_{q_0}(x_1)| + \log b\,|R_1(x_1)|.$$

How can Φ_b be chosen? The argument asks for a second property, which pulls against density: for every small prime ℓ, it restricts which signed powers of ℓ can occur as ratios of labels of b-places after reduction modulo the prime-to-ℓ part of q_1. Behrend's construction [Beh] meets both: lattice points on a sphere, written as digits in a large base, become exponents of one element of U_{q_1}.

Throughout, for $q' \mid q_1$ let $\mathrm{cl}_{q'} \colon \Phi \to U_{q'}$ be the label reduced modulo q', so that $\mathrm{cl} = \mathrm{cl}_{q_0}$; for a prime ℓ let $q_{(\ell)}$ be the largest divisor of q_1 prime to ℓ. For the parameters (q_0, d) and an integer $s \geq 0$, Chapter 33 sets

$$l_0(s) = 3^{\lfloor \log_3 s \rfloor + 4}, \qquad q_1 = q_0 \cdot 3\, l_0(s)\, 2^s,$$

with $\lfloor \log_3 0 \rfloor$ read as 0. With $e := \lfloor \log_3 s \rfloor$ this is the $q_1 = q_0\, 3^{e+5} 2^s$ of Chapter 3, and Problem 3.1.3 gives $\#\Phi_a = q_1/q_0 = 3l_0(s)2^s$. We write l_0 when s is fixed. Exponents in group powers and congruences are integers, as are the exponents in prime-power moduli.

4.1. Two requirements

The first requirement is size, measured against the class of -1.

Problem 4.1.1. Multiplication by $[-1]$ maps Φ_a bijectively onto $\mathrm{cl}^{-1}(-1)$, so $\mathrm{cl}^{-1}(-1)$ has $\#\Phi_a$ elements. In the toy example of Chapter 3, $q_0 = 4$, $q_1 = 16$, it consists of the places with labels $3, 7, 11, 15$.

An admissible datum (Chapter 33) requires

$$q_1/q_0 \leq \#\Phi_b \log b, \tag{1}$$

so Φ_b must contain at least the proportion $1/\log b$ of $\mathrm{cl}^{-1}(-1)$.

The second requirement concerns ratios of places. For $\ell \nmid q_1$, the label of $[\ell]$ is $\ell \bmod q_1$. For $\ell \mid q_1$, the convention of Chapter 3 makes $[\ell]$ the identity. In both cases the sparsity condition compares the reduced label of a ratio with signed powers of ℓ modulo $q_{(\ell)}$.

Date: November 26, 2026.

Problem 4.1.2. Let ℓ be a prime, $\sigma \in \Phi$ and $i \geq 1$. (i) If $\ell \nmid q_1$, then $q_{(\ell)} = q_1$, and the places τ with $\mathrm{cl}_{q_{(\ell)}}(\tau/\sigma) = \pm\ell^i$ are the two places $[\pm\ell^i]\sigma$. (ii) If $\ell^\nu \| q_1$ with $\nu \geq 1$, then for each sign there are $\ell^{\nu-1}(\ell-1)$ such places. For $q_1 = 36$, $\ell = 3$ this is 6.

The proof states the second requirement as follows. For a natural number L, a finite set $\mathcal{P} \subseteq \Phi$ is *sparse for the primes up to* L if for every prime $\ell \leq L$ and all integers $0 < i < i' < l_0(s)$ there are no $\sigma, \tau, \tau' \in \mathcal{P}$, distinct or not, and no signs $\varepsilon, \varepsilon' \in \{\pm 1\}$ with

$$\mathrm{cl}_{q_{(\ell)}}(\tau/\sigma) = \varepsilon\,\ell^i \quad \text{and} \quad \mathrm{cl}_{q_{(\ell)}}(\tau'/\sigma) = \varepsilon'\ell^{i'} \quad \text{in } \mathbb{Z}/q_{(\ell)}\mathbb{Z}.$$

An admissible datum requires Φ_b to be sparse for the primes up to kt, where $k = r + 1 - m$ and $t = 5r$, with m the number of lifts and r the rank of the target (Chapter 33).

Problem 4.1.3. Let $\mathcal{P}$ be sparse for the primes up to L, let $\ell \leq L$ be prime, $v \in U_{q_{(\ell)}}$, and choose a sign ε_μ for every integer μ. Among any l_0 consecutive integers μ, at most two have $\varepsilon_\mu \ell^\mu v \in \mathrm{cl}_{q_{(\ell)}}(\mathcal{P})$.

Problem 4.1.4. Let $\mathcal{P}$ be sparse for the primes up to L, let $p \leq L$ be a prime with $p \nmid q_1$, and $0 < i < i' < l_0$. For no σ are all three of σ, $[-p]^i\sigma$, $[-p]^{i'}\sigma$ in $\mathcal{P}$.

The sparsity of Φ_b is used in two places. Chapter 19 uses Problem 4.1.4 for Φ_b when $p \leq k$ and $\chi_K(p) \neq 1$, in the sharpness argument for the divisibility of derivatives (Problem 19.4.3 and the paragraph before it). The condition $\chi_K(p) \neq 1$ implies $p \nmid q_1$, since every prime divisor of q_1 divides q_0 and Problem 3.1.6(i) applies. Chapter 67, Section 67.2, states the bound $4f\,\mathrm{defect}_\ell$ per unit of rank for the local defect above ℓ; at primes $\ell \leq kt$ the local argument behind it uses sparsity to exclude a third b-place on a short arc. That chapter omits the local argument.

Why are the two requirements in tension? We shall look for Φ_b among the places $[-g^n]$ for the integer g of Section 4.3, whose order modulo a power of 2 is 2^s (Problem 4.3.2). Section 4.3 uses a set of exponents $\mathcal{N} \subseteq [0, 2^s)$ with the following property: for all $n_1, n_2, n_3 \in \mathcal{N}$ and positive integers α, α' with $\alpha + \alpha' \leq 2l_0$, the congruence $(\alpha + \alpha')n_2 \equiv \alpha n_1 + \alpha' n_3 \pmod{2^s}$ implies $n_1 = n_2 = n_3$. For $\alpha = \alpha' = 1$ this excludes nonconstant three-term progressions. The obvious sets without them are thin.

Problem 4.1.5. For an integer $\mu \geq 0$, let $\mathcal{N}_\mu$ be the set of integers in $[0, 3^\mu)$ whose base-3 digits are 0 or 1. (i) $\mathcal{N}_\mu$ contains no nonconstant three-term arithmetic progression, and $|\mathcal{N}_\mu| = (3^\mu)^{\log 2/\log 3}$. (ii) For $\mu \geq 2$, $\mathcal{N}_\mu$ contains $0, 1, 3$, and $3 \cdot 1 = 2 \cdot 0 + 1 \cdot 3$, a relation with $\alpha = 2$, $\alpha' = 1$.

We compare the expected size of a random set with its expected number of progressions.

Problem 4.1.6. Let $o \geq 4$ be even, and let $R \subseteq \mathbb{Z}/o\mathbb{Z}$ contain each element independently with probability δ. The expected number of pairs (n, η) with $\eta \notin \{0, o/2\}$ and $n, n+\eta, n+2\eta \in R$ is $o(o-2)\delta^3$. If $\delta^2(o-2) > 1$, this exceeds the expected size δo of R.

Problem 4.1.7. Let R be as in Problem 4.1.6. For each pair (n, η) counted there choose one of $n, n+\eta, n+2\eta$, and let R' be obtained from R by deleting the chosen points. Then R' contains no three distinct points $n, n+\eta, n+2\eta$, and its expected size is at least $\delta o - \delta^3 o^2$. For $\delta \leq (2o)^{-1/2}$ this is at least $\delta o/2$.

For an admissible datum let $o = 2^s$. Then $o = m^{22}$, $\sqrt{x} \le m \le 2\sqrt{x}$ and $(\log b)^{100} \le x$ (Chapter 33). The density guaranteed by Problem 4.1.7 is of order $o^{-1/2}$ at best, and $(2o)^{-1/2} < x^{-5}$. For places indexed injectively by exponents modulo o, (1) asks for an exponent density at least $3l_0/\log b > x^{-1/100}$. The deletion estimate falls short of the required density by a power of x. We now choose the exponents using lattice points on a sphere.

4.2. Behrend's construction

Behrend [Beh] encodes lattice points of fixed squared length by their digits. Let $D, H \ge 1$ be integers and $\Sigma_\rho := \{v \in \{0, \dots, H-1\}^D : |v|^2 = \rho\}$.

Problem 4.2.1. Let $v, v', v'' \in \mathbb{Z}^D$ have $|v|^2 = |v'|^2 = |v''|^2$, and let α, α' be positive integers with $(\alpha + \alpha')v' = \alpha v + \alpha' v''$. Then $v = v' = v''$.

Problem 4.2.2. Some ρ has $|\Sigma_\rho| \ge H^D/(DH^2)$.

Fix such a ρ and an integer $Q \ge 1$. Let $\beta := QH$, $\mathrm{enc}(v) := \sum_{\mu=0}^{D-1} v_\mu \beta^\mu$, and $\mathcal{N} := \mathrm{enc}(\Sigma_\rho)$.

Problem 4.2.3. If $z_0, \dots, z_{D-1}$ are integers with $|z_\mu| < \beta$ and $\sum_\mu z_\mu \beta^\mu = 0$, then every $z_\mu = 0$. In particular enc is injective on $\{0, \dots, H-1\}^D$.

Problem 4.2.4. Let $n_1, n_2, n_3 \in \mathcal{N}$, and let α, α' be positive integers with $\alpha + \alpha' \le Q$. If $(\alpha + \alpha')n_2 = \alpha n_1 + \alpha' n_3$, then $n_1 = n_2 = n_3$.

Problem 4.2.5. For $D = 3$, $H = 3$, $Q = 8$, so $\beta = 24$, the sphere with the most points is $\rho = 5$, with the six permutations of $(0, 1, 2)$, and $\mathcal{N} = \{26, 49, 578, 624, 1153, 1176\}$. With $Q = 6$, $\beta = 18$, the same sphere gives $\{20, 37, 326, 360, 649, 666\}$.

Problem 4.2.6. Let $o \ge \beta^D$ be an integer. (i) Every $n \in \mathcal{N}$ satisfies $n < o$. (ii) For $n_1, n_2, n_3 \in \mathcal{N}$ and positive integers α, α' with $\alpha + \alpha' \le Q$, the congruence $(\alpha + \alpha')n_2 \equiv \alpha n_1 + \alpha' n_3 \pmod{o}$ implies $n_1 = n_2 = n_3$.

Problems 4.2.1–4.2.4 and 4.2.6 give the following theorem for $D, H \ge 1$; the statement in the proof also covers $DH = 0$. Here D, H, Q, o are natural numbers, and the quotient $H^D/(DH^2)$ is taken in $\mathbb{R}$, with value 0 when $DH = 0$.

Theorem 4.2.1. *If $0 < Q$ and $(QH)^D \le o$, there is a finite set $\mathcal{N}$ of natural numbers such that $n < o$ for every $n \in \mathcal{N}$, $H^D/(DH^2) \le \#\mathcal{N}$, and for all $n_1, n_2, n_3 \in \mathcal{N}$ and all natural numbers α, α' with $0 < \alpha$, $0 < \alpha'$, $\alpha + \alpha' \le Q$, the congruence $(\alpha + \alpha')n_2 \equiv \alpha n_1 + \alpha' n_3 \pmod{o}$ implies $n_1 = n_2$ and $n_2 = n_3$.*

For $Q = 2$, the first Exercise below gives the density lower bound $\exp(-C\sqrt{\log o})$ of Behrend's construction [Beh]. No construction gives a density bounded below by a positive constant independent of N: by Roth's theorem [Ro] a set of integers in $[0, N)$ without nonconstant three-term progressions has $o(N)$ elements as $N \to \infty$. The size condition we need is (1).

4.3. From exponents to places

The exponents of Theorem 4.2.1 become places through one integer g prime to q_1. Let $w = v_2(q_0)$, so that $2^{s+w} \mid q_1$; since $16 \mid 18480$, $w \ge 4$, and the problems below use only $w \ge 2$. Following the construction of the proof, let

$$g := 1 + 3l_0q_0, \qquad \sigma_n := [-g^n] \in \Phi \quad (n \ge 0).$$

A toy of the same shape has $q_0 = 4$ and $l_0 = 3$ in place of the values of the proof, and $s = 13$: then $q_1 = 4 \cdot 9 \cdot 2^{13} = 294912$, $w = 2$ and $g = 37$. In the toy the prime 3 divides q_1 but not q_0, which nothing below uses, and "sparse" is taken with $l_0 = 3$.

Problem 4.3.1. (i) If $c \geq w \geq 2$ and y is odd, then $1 + 2^w y$ has order 2^{c-w} in U_{2^c}. (ii) If $c \geq 1$, then 4 has order 3^{c-1} in U_{3^c}. For example $5^0, 5^1, 5^2, 5^3 \equiv 1, 5, 9, 13 \pmod{16}$, and 4 has order 3 modulo 9.

Problem 4.3.2. The integer g has order 2^s modulo 2^{s+w}. The places σ_n, $0 \leq n < 2^s$, are distinct, and their labels are $\equiv -1 \pmod{3 l_0 q_0}$, in particular modulo q_0. In the toy, 37 has order 2^{13} modulo 2^{15}.

Problem 4.3.3. Let $0 < i < l_0$ and $n, n' \geq 0$. Then $\mathrm{cl}_{q_{(2)}}(\sigma_{n'}/\sigma_n) \neq \pm 2^i$.

Problem 4.3.4. Let ℓ be an odd prime, $0 < i < i'$, and $n_1, n_2, n_3 \geq 0$. If $\mathrm{cl}_{q_{(\ell)}}(\sigma_{n_2}/\sigma_{n_1}) = \pm \ell^i$ and $\mathrm{cl}_{q_{(\ell)}}(\sigma_{n_3}/\sigma_{n_1}) = \pm \ell^{i'}$, then

$$2i'\, n_2 \equiv 2(i' - i)\, n_1 + 2i\, n_3 \pmod{2^s}.$$

Problem 4.3.5. Let $\ell > 1$ be an odd integer, $\lambda \geq 1$ and $s \geq 0$. If $\ell^\lambda \equiv 1 \pmod{2^{s+1}}$, then $2^s \leq (\ell + 1)\lambda$.

Problem 4.3.6. In the toy, the places σ_n for $n = 20, 37, 326, 360, 649, 666$ have labels 153935, 39851, 74807, 243359, 190331, 43271 modulo 294912. These are $\equiv -1 \pmod{36}$, and the six places form a set sparse for the primes up to 1364, the largest L with $6(L + 1) < 2^{13}$.

Problems 4.3.2–4.3.5, with Theorem 4.2.1 for $Q = 2l_0$ and $o = 2^s$, prove the next theorem. It concerns the parameters (q_0, d) and natural numbers s, D, H, L, with the same convention for $H^D/(DH^2)$ as in Theorem 4.2.1.

Theorem 4.3.1. *If $(2l_0(s)H)^D \leq 2^s$ and $2l_0(s)(L + 1) < 2^s$, there is a finite set $\mathcal{P} \subseteq \Phi$ with $\mathrm{cl}(\sigma) = -1$ for every $\sigma \in \mathcal{P}$, with $H^D/(DH^2) \leq \#\mathcal{P}$, and sparse for the primes up to L.*

It remains to choose D and H so that $\#\mathcal{P}$ is large compared with q_1/q_0.

Problem 4.3.7. Let $D \geq 1$ be an integer and $W \geq 1$ real, with $W \leq 2^s \leq W^D$, $(2l_0)^D \leq W$ and $3l_0 D 2^D \leq W^3$, and let H be the largest power of 2 with $H^D \leq 2^s/W$. Then $H \leq W$, $(2l_0 H)^D \leq 2^s$, and $q_1/q_0 \leq W^6 H^D/(DH^2)$.

With Theorem 4.3.1 this gives a set of places of class -1 modulo q_0, sparse for the primes up to L, with $q_1/q_0 \leq \#\mathcal{P} \cdot W^6$, under the hypotheses of Problem 4.3.7 and $2l_0(L + 1) < 2^s$. If moreover $W^6 \leq \log b$, then $\mathcal{P}$ satisfies (1) in place of Φ_b. This ends the choice of places. From Chapter 5 on, the next part develops the comparison of divisibility with size.

In the Lean formalization. In the Lean proof [GL], sparsity is the definition `New.Parameters.IsSparse` (file `New/Reduction/Data/AdmissibleData.lean`), and Theorems 4.2.1 and 4.3.1 are `New.exists_three_term_free` and `New.Parameters.exists_large_isSparse` (file `New/Reduction/Data/Existence.lean`); the proof of the latter is the construction of Section 4.3.

Exercises.

(1) With $Q = 2$, $D = \lceil \sqrt{\log o} \rceil$ and H the largest integer with $(2H)^D \leq o$, Theorem 4.2.1 gives a set $\mathcal{N} \subset [0, o)$ without nonconstant three-term progressions modulo o and with $\#\mathcal{N} \geq o \exp(-C\sqrt{\log o})$ for large o, for an absolute constant C.

(2) The hypothesis $o \geq \beta^D$ cannot be dropped from Problem 4.2.6: for $D = 3$, $H = Q = 2$, $\rho = 1$ and $o = 27$, every element of $\mathcal{N}$ is less than o, but three distinct elements of $\mathcal{N}$ form an arithmetic progression modulo o.

Hints

§4.1.

4.1.1: Problem 3.1.3.
4.1.2: (ii) Count a fibre of $U_{q_1} \to U_{q_{(\ell)}}$.
4.1.3: Take three such μ.
4.1.4: $(-p)^i = (-1)^i p^i$.
4.1.5: (i) Add the outer terms digit by digit.
4.1.6: For $\eta \notin \{0, o/2\}$ the three points are distinct.
4.1.7: Linearity of expectation.

§4.2.

4.2.1: Three distinct points of a sphere are never collinear. Compute $\alpha|v|^2 + \alpha'|v''|^2 - (\alpha + \alpha')|v'|^2$ in terms of $v - v''$.
4.2.2: Count the possible values of $|v|^2$.
4.2.3: Look at the lowest nonzero z_μ modulo β.
4.2.4: Problem 4.2.3.
4.2.6: (ii) Bound the base-β digits of both sides.

§4.3.

4.3.1: Induction on the exponent of 2, resp. 3, in $(1+2^w y)^{2^r} - 1$, resp. $4^{3^r} - 1$.
4.3.2: Problem 4.3.1(i).
4.3.3: Use $3l_0 \mid q_{(2)}$ and Problem 4.3.1(ii).
4.3.4: For odd ℓ, $2^{s+w} \mid q_{(\ell)}$. Work modulo 2^{s+w}.
4.3.5: Compute $v_2(\ell^\lambda - 1)$ for λ odd and for λ even; for λ even use $\ell^2 - 1 = (\ell - 1)(\ell + 1)$ and Problem 4.3.1(i) for ℓ^2.
4.3.6: Problems 4.2.5 (base 18), 4.3.3 and 4.3.4 with $l_0 = 3$; if the exponents coincide, Problem 4.3.5.
4.3.7: Compare $(2H)^D$ with $2^s/W$.

References

[Beh] F. A. Behrend, *On sets of integers which contain no three terms in arithmetical progression*, Proc. Nat. Acad. Sci. U.S.A. **32** (1946), 331–332.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer, 1990.

[Ro] K. F. Roth, *On certain sets of integers*, J. London Math. Soc. **28** (1953), 104–109.