The Farey Series of polynomials over a finite field

Autor(en): **Webb, William A.**

Objekttyp: **Article**

Zeitschrift: **Elemente der Mathematik**

Band (Jahr): **41 (1986)**

Heft 1

PDF erstellt am: **24.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-39465

den. In diesem Fall erweist sich k_2 als einfache Kurve und δ_2 fällt mit dem Tangentendrehwinkel von k_A zusammen.

Helmut Pottmann, TU Wien

LITERATURVERZEICHNIS

1 W. Blaschke und H. R. Müller: Ebene Kinematik. Oldenbourg, München 1956.
2 L. Hering: Sätze vom Holditch-Typ für ebene Kurven. El. Math. *38*, 39–49 (1983).
3 H. Holditch: Geometrical Theorem. Q. J. Pure Appl. Math. *2* (1858).
4 H. R. Müller: Kinematik. Sammlg. Göschen (Bd. 584/584a), Berlin 1963.
5 H. Pottmann: Holditch-Sicheln. Arch. Math. *44*, 373–378 (1985).
6 H. Pottmann: Ein isotropes Analogon zum Satz von Holditch. J. of Geometry (im Druck).
7 W. Wunderlich: Ebene Kinematik. Bibl. Inst. HTB (Bd. 447/447a), Mannheim/Wien/Zürich 1970.

 0013-6018/86/060001-06$1.50 + 0.20/0

The Farey series of polynomials over a finite field

Introduction

The ordinary Farey series of order n, $F_n = \{h/k | 0 \leq h \leq k \leq n, (h,k) = 1\}$ has a number of interesting intrinsic properties as well as having applications to such diverse areas as approximating irrational numbers, solving the Diophantine equation

$$a/b = 1/x_1 + \cdots + 1/x_k$$

(Egyptian fraction problem), and the Hardy-Littlewood method of analytic number theory.
If p is a prime, let $GF(p^r)$ be the finite field with p^r elements, and $GF[p^r, x]$ the ring of polynomials over this field. The Farey series $\mathfrak{F}_n$ is defined as:

$$\mathfrak{F}_n = \{P/Q | P, Q \in GF[p^r, x], \quad \deg P < \deg Q \leq n, \quad (P,Q) = 1, \quad Q \text{ monic}\}.$$

We let $GF(p^r, x)$ denote the field of rational functions over $GF(p^r)$; $v(P/Q) = \deg Q - \deg P$ the usual degree valuation on $GF(p^r, x)$; $GF\{p^r, x\}$ the completion of $GF(p^r, x)$ with respect to v, so

$$GF\{p^r, x\} = \left\{\alpha = \sum_{j=t}^{\infty} a_j x^{-j} | a_j \in GF(p^r)\right\}$$

where $v(\alpha) = t$ and $|\alpha| = (p^r)^{-v(\alpha)} = p^{-rt}$. (The degree of the zero polynomial is taken to be $-\infty$.) Also, the distance between α und β is given by $|\alpha - \beta|$, which is easily seen to be an ultrametric on $GF\{p^r, x\}$. The set $\mathfrak{I} = \{\alpha | v(\alpha) > 0\}$ consists of all elements of the form

$\sum_{j=1}^{\infty} a_j x^{-j}$ and corresponds to the unit interval [0, 1] in the reals. Indeed in [3] Hayes uses $\mathfrak{F}_n$ to define what he calls a primordial subdivision of $\mathfrak{I}$ which corresponds to the Farey dissection of [0, 1], in order to develop an analog of the Hardy-Littlewood method to apply to additive problems in $GF[p^r, x]$.

Elementary properties

In what follows, we will develop some other properties of $\mathfrak{F}_n$ which correspond to some of the well-known properties of F_n. It will be seen that there are many striking similarities as well as some significant differences in the two kinds of Farey series.
The idea of consecutive fractions in F_n plays a central role in many of the elementary properties. Since $\mathfrak{F}_n$ is not linearly ordered, we cannot speak of consecutive elements, so we consider neighboring elements instead. We will define neighbors in $\mathfrak{F}_n$ as fractions which are close to each other. The possible distances between fractions in either F_n or $\mathfrak{F}_n$ depends heavily on the size of the denominators. We will thus refer to $P/Q \in \mathfrak{F}_n$ as an element of degree q if $q = \deg Q$.

Definition. *Given P/Q in $\mathfrak{F}_n$ the element $H/K \neq P/Q$ in $\mathfrak{F}_n$ where $k = \deg K$, is a k-neighbor of P/Q if $|P/Q - H/K| \leq |P/Q - H'/K'|$ for all H'/K' of $\deg k$.*

Although this definition is useful in that it specifies the degree of a neighbor, the relation is not symmetric. For example, $(x + 1)/(x^2 + x + 1)$ is a 2-neighbor of $x^2/(x^3 + 1)$ but $x^2/(x^3 + 1)$ is not a 3-neighbor of $(x + 1)/(x^2 + x + 1)$. Hence, we will also use:

Definition. *The fractions P/Q, $H/K \in \mathfrak{F}_n$, $\deg Q = q$, $\deg K = k$ are neighbors, if P/Q is a q-neighbor of K and H/K is a k-neighbor of P/Q.*

Lemma 1. *If $P/Q \in \mathfrak{F}_n$, define X and Y by $PX - QY = 1$, $\deg X < \deg Q$, $\deg Y < \deg P$. Then $\deg(HQ - KP) = 0$ if and only if $H = aY + AP$ and $K = aX + AQ$ where $a \neq 0$, $a \in GF(p^r)$ and $A \in GF[p^r, x]$.*

Proof: $(aY + AP)Q - (aX + AQ)P = a(QY - PX) = -a$. Conversely, if $HQ - KP = -a \neq 0$ then $PK \equiv a \pmod{Q}$ which implies $K \equiv aX \pmod{Q}$. Letting $K = aX + AQ$, we have $a = P(aX + AQ) - HQ = a(1 + QY) + PAQ - HQ = a + Q(aY + AP - H)$ so $H = aY + AP$. Note that $(H, K) = 1$, and for $A \neq 0, K$ is monic if and only if A is monic.
In what follows, q_i will always denote the degree of Q_i.

Theorem 1. *P_1/Q_1 and P_2/Q_2 in $\mathfrak{F}_n$ are neighbors if and only if $\deg(P_1Q_2 - P_2Q_1) = 0$.*

Proof: If $\deg(P_1Q_2 - P_2Q_1) = 0$ then P_1/Q_1 and P_2/Q_2 are clearly neighbors since

$$\left|\frac{P_1}{Q_1} - \frac{P_2}{Q_2}\right| = p^{-r(q_1 + q_2)}$$

is minimal.

Conversely, we may assume $q_1 \leq q_2$ and P_2/Q_2 is a q_2-neighbor of P_1/Q_1. By taking A in Lemma 1 to be any monic polynomial of degree $q_2 - q_1$ (so $A = 1$ if $q_1 = q_2$) there exists an H/K of degree q_2 such that $|H/K - P_1/Q_1| = p^{-r(q_1+q_2)}$. Therefore

$$\frac{P_1}{Q_1} - \frac{P_2}{Q_2} \leq p^{-r(q_1+q_2)}$$

which implies $\deg(P_1 Q_2 - P_2 Q_1) = 0$.

Theorem 2. *If $P/Q \in \mathfrak{F}_n$ then P/Q has exactly $(p^r - 1)p^{rt}$ neighbors of degree $q + t$ for $t \geq 0$, and exactly one neighbor of degree less than q.*

Proof: By the previous two results, the neighbors of P/Q are precisely the polynomials of the form: $H = aY + AP, K = aX + AQ$.

If $\deg K = q + t$ then A can be any monic polynomial of degree t and $a \neq 0$.
If $\deg K < \deg Q$ then $A = 0$ and a must be chosen so that aX is monic.

We therefore have an easy way to construct $\mathfrak{F}_n$ given $\mathfrak{F}_{n-1}$. By Theorem 2, $\mathfrak{F}_n$ consists of $\mathfrak{F}_{n-1}$ and all n-neighbors of the elements in $\mathfrak{F}_{n-1}$, which are easily found as described in the proof.
This remark also allows a very simple induction proof of the following result which is necessary for the primordial subdivision of $\mathfrak{I}$ [1], [3].

Proposition. *If $\Phi(k)$ denotes the number of polynomials H in a reduced residue system modulo K, then*

$$\sum_{\substack{\deg K = k \\ K \text{ monic}}} \Phi(K) = \begin{cases} p^{2rk} - p^{2rk-r} & \text{for } k > 0, \\ 1 & \text{for } k = 0. \end{cases}$$

Proof: The case $k = 0$ is obvious. Clearly the sum in question counts the number of elements of $\mathfrak{F}_n$ of degree $k \leq n$. Hence,

$$\begin{aligned} \sum_{\substack{\deg K = k \\ K \text{ monic}}} \Phi(K) &= \sum_{h=0}^{k-1} \sum_{\substack{\deg H = h \\ H \text{ monic}}} \Phi(H)(p^r - 1)p^{r(k-h)} \\ &= (p^r - 1)p^{rk}\left(\sum_{h=1}^{k-1} p^{-rh}(p^{2rh} - p^{2rh-r}) + 1\right) \\ &= (p^r - 1)p^{rk}(p^{r(k-1)} - 1 + 1) = p^{2rk} - p^{2rk-r}. \end{aligned}$$

So far we have discussed only neighboring pairs. But since $GF(p^r, x)$ is not linearly ordered we may also have sets of fractions which are all mutual neighbors.
Suppose $\{P_i/Q_i\}$ is a set of at least three mutual neighbors. We will look for maximal such sets.

By Theorem 2 the set $\{P_i/Q_i\}$ cannot contain elements having 3 different degrees, indeed all of the elements must be of the same degree except possibly for one of smaller degree. Choose one of the elements having the larger degree, say P_1/Q_1 and call it P/Q. Since P/Q has $p^r - 1$ neighbors of degree q, a maximal set of mutual neighbors contains at most p^r elements of degree q and one element of degree $< q$. We will show that maximal sets are indeed of this form.

Using the notation of Lemma 1, with subscripts where appropriate, the only possible elements of $\{P_i/Q_i\}$ are P/Q, Y/X and $(aY + P)/(aX + Q)$ for $a \in GF(p^r)$, where X and Y are normalized so that X is monic. It is routine to check that these elements are indeed mutual neighbors, since for example $(a_1 Y + P)(a_2 X + Q) - (a_2 Y + P)(a_1 X + Q) = a_1(YQ - XP) + a_2(XP - YQ) = a_2 - a_1 \in GF(p^r)$. We have thus proved:

Theorem 3. *Every set of mutual neighbors in $\mathfrak{F}_n$ is a subset of some set of the form*

$$\{Y/X, (aY + P)/(aX + Q) \text{ for } a \in GF(p^r)\} \text{ where } P/Q \in \mathfrak{F}_n,$$
$$PX - QY = 1;\ \deg X < \deg Q;\ \deg Y < \deg P;\ Q, X \text{ monic}.$$

Approximating nonrational functions

As previously mentioned the development of the Hardy-Littlewood method for $GF[p^r, x]$ in [3] involved a decomposition of $\mathfrak{I}$. This decomposition consists of all sets of the form $\{Z \in GF\{p^r, x\} | v(Z - P/Q) \geq q + n + 1\}$ for all $P/Q \in \mathfrak{F}_n$.

Hence, the following result is immediate.

Theorem. *If $\alpha \in \mathfrak{I}$ and n is a positive integer, then there is an element $P/Q \in \mathfrak{F}_n$ such that*

$$|\alpha - P/Q| \leq \frac{1}{p^{r(q+n+1)}}.$$

Corollary. *If $\alpha \in \mathfrak{I}$ and α is not a rational function, then there are infinitely many rational functions P/Q such that*

$$|\alpha - P/Q| \leq \frac{1}{p^{r(2q+1)}}.$$

These results correspond to the elementary results about real numbers (1) $|x - a/b| \leq 1/b(n + 1)$ and (2) $|x - a/b| \leq 1/b(b + 1) < 1/b^2$. For real numbers, (2) is not the best possible result and the bound $1/b^2$ can be replaced by $1/2b^2$ with a little more care, and by $1/\sqrt{5}b^2$ with even more care. However, the above Corollary is the best possible result for $\mathfrak{I}$, as the following example shows.

It is easily seen that $\sqrt{x^2 + 4}$ is in $GF\{p^r, x\}$ and has an expansion

$$\sqrt{x^2 + 4} = x + 2/x + \cdots (p \neq 2)$$

so $\alpha = \sqrt{x^2 + 4} - x \in I$, and $v(\alpha) = -1$. Also α is not rational.

Suppose $|\alpha - P/Q| \leq p^{-r(2q+2)}$ or $v(\alpha - P/Q) \geq 2q + 2$. Let $\beta = \alpha - P/Q$. Then $\sqrt{x^2+4} - \beta = P/Q + x$ so $Q(\sqrt{x^2+4} - \beta) = P + xQ \in GF[p^r, x]$.
Hence, $Q^2(x^2 + 4 - 2\beta\sqrt{x^2+4} + \beta^2) \in GF[p^r, x]$ which implies $Q^2\beta^2 - 2Q^2\beta\sqrt{x^2+4} \in GF[p^r, x]$. But $v(Q^2\beta^2) \geq -2q + 2(2q+2) = 2q + 4$ and $v(2Q^2\beta\sqrt{x^2+4}) \geq -2q + (2q+2) - 1 = 1$, which means $Q^2\beta^2 - 2Q^2\beta\sqrt{x^2+4}$ cannot be a polynomial. Hence $|\alpha - P/Q| \leq p^{-r(2q+1)}$ is the best approximation possible.

Egyptian fractions

The problem of expressing rational numbers a/b as a sum of reciprocals of distinct integers is an old one with an extensive literature. Recently, Dobbs and McConnel [2] discussed an algorithm for solving the same problem in the ring $K(x)$ where K is a field. The algorithm used is closely related to the Fibonacci algorithm. (This algorithm was first used by Fibonacci ca. 1202, but is not related to the Fibonacci numbers.) Several other algorithms for the integer problem are known, including one based on the Farey series. The same type of algorithm also exists in $GF(p^r, x)$.
Given a nonzero element in $GF(p^r, x)$ expressed as P_1/Q_1 where $P_1, Q_1 \in GF[p^r, x]$, we wish to express P_1/Q_1 in the form:

$$\frac{P_1}{Q_1} = \frac{1}{H_1} + \frac{1}{H_2} + \cdots + \frac{1}{H_k}, \quad H_j \in GF[p^r, x], \qquad H_i \neq H_j \quad \text{for} \quad i \neq j.$$

It is easily checked that the condition $\deg P_1 < \deg Q_1$ is necessary [2]. Also, we may assume without loss of generality that $(P_1, Q_1) = 1$ and Q_1 is monic.
Then P_1/Q_1 is an element of some $\mathfrak{F}_n$ ($\mathfrak{F}_{q_1}$ in particular), so by Lemma 1 and Theorem 2, P_1/Q_1 has a neighbor Y_1/X_1, $\deg Y_1 < \deg X_1 < \deg Q_1$, $\deg Y_1 < \deg P_1$ and

$$\frac{P_1}{Q_1} = \frac{Y_1}{X_1} + \frac{P_1X_1 - Q_1Y_1}{Q_1X_1} = \frac{Y_1}{X_1} + \frac{1}{Q_1X_1} = \frac{P_2}{Q_2} + \frac{1}{Q_1Q_2}$$

where $P_2 = Y_1$ and $Q_2 = X_1$. Repeat this procedure successively with $P_2/Q_2, P_3/Q_3, \ldots$ until we encounter $\deg Y_j = 0$. This must occur in at most $\deg P_1$ steps since $\deg Y_j < \deg P_j < \deg P_{j-1} < \cdots < \deg P_1$. Thus,

$$\frac{P_1}{Q_1} = \frac{1}{Q_1Q_2} + \frac{1}{Q_2Q_3} + \cdots + \frac{1}{Q_{j-1}Q_j} + \frac{1}{Q_jQ_{j+1}} + \frac{1}{Q^*_{j+1}}$$

where $Y_j/X_j = 1/Q^*_{j+1}, Q^*_{j+1} = cQ_{j+1}$, for some $c, c \in GF(p^r)$. The fractions $1/Q_iQ_{i+1}$ are distinct since

$$\deg(Q_1Q_2) > \deg(Q_2Q_3) > \cdots > \deg(Q_jQ_{j+1}) > \deg Q^*_{j+1}.$$

Of particular interest in Egyptian fraction problems are questions concerning such things as the number of terms or the size of the terms in the expansion. If $\deg P = n$ then both the Farey series algorithms given above, and the algorithm given by Dobbs and McConnel

yield an expansion of length at most $n + 1$. Over the integers, the related algorithms both yield expansions for a/b of length at most a.
However, the algorithms differ greatly in size of the terms produced. The largest degree term produced by the Farey series algorithm is clearly $1/Q_1 Q_2$ which has degree at most $2q_1 - 1$ since $\deg Q_2 < \deg Q_1 = q_1$. The Fibonacci type algortihm yields a bound depending on both degrees of P and Q. In the worst case, where $\deg P = q - 1$, the largest term may have degree as large as $2^{q_1 - 1}$. This behavior again mirrors that of the related algorithms over the ordinary integers.

William A. Webb, Department of Mathematics
Washington State University

REFERENCES

1 L. Carlitz: Representations of arithmetic functions in $GF[p^r, x]$. Duke Math. J. *14*, 1121–1137 (1947).
2 D. Dobbs and R. McConnel: An Egyptian algorithm for polynomials. El. Math. *39*, 126–129 (1984).
3 D. R. Hayes: The expression of a polynomial as a sum of three irreducibles. Acta Arith. *11*, 461–488 (1966).

 0013-6018/86/060006-06$1.50 + 0.20/0

Kleine Mitteilungen

Über eine Vermutung von Thébault

Die hier behandelte Aufgabe wurde 1938 von V. Thébault in [2] gestellt und erschien in beiden Auflagen von C. Stanley Ogilvys Buch «Tomorrow's Math., Unsolved Problems for the Amateur» (Oxford University Press: 1962, p. 70; 1972, p. 82). Erst 45 Jahre später fand K. B. Taylor eine Lösung, die aber wegen ihrer beträchtlichen Länge (24 Seiten) nur in Form eines knappen Auszugs abgedruckt wurde [1]. In der vorliegenden Note soll ein kurzer Beweis gegeben werden.

Satz. *Es sei T ein beliebig gewählter Punkt auf der Seite c des Dreiecks ABC. (M_1, r_1) bzw. (M_2, r_2) seien die Kreise, die AT, TC bzw. BT, TC und den Umkreis (von innen) berühren. Ist I der Mittelpunkt des Inkreises und r sein Radius, dann liegen M_1, M_2 und I kollinear. Bezeichnet θ die Hälfte des Winkels ATC, dann gilt weiter $\overline{M_1 I} : \overline{I M_2} = \sin^2\theta : \cos^2\theta$ und* $r_1 \cos^2\theta + r_2 \sin^2\theta = r$.
(Anstelle von $r_1 \cos^2\theta + r_2 \sin^2\theta = r$ wurde von Thébault (und Ogilvy) fälschlich $r_1 + r_2 = r^2 \sec^2\theta$ angegeben; vgl. [1].)

Beweis: P_1 sei der Schnittpunkt von AB mit dem Lot durch I auf die innere Winkelsymmetrale des Winkels ATC, und M_1 sei der Schnittpunkt des Lotes durch P_1 auf AB mit dieser Winkelsymmetralen; M_2 ist analog zu definieren. Der Kreis mit Mittelpunkt M_1 und Radius $r_1 = \overline{M_1 P_1}$ berührt dann AT und TC. Es bleibt nachzuweisen, dass er auch den Umkreis (von innen) berührt; dies ist äquivalent zu $\overline{UM_1} = R - r_1$, wobei R den