

1 Notes from 31 Oct 2006

1.1 Theorem Let $n \geq 1$ be an odd integer and r a prime, $r \nmid n$, such that the order of n in $(\mathbb{Z}/r)^*$ is at least $4(\log n)^2$ and such that $(x+a)^n = x^n + a$ in $R_n := \mathbb{Z}/n[x]/(x^r - 1)$ for all a with $1 \leq a \leq 2\sqrt{r}(\log n)$.

Then n is a prime power.

Proof: We will proceed via a series of Lemmas.

Let $p \mid n$ be prime and set $l = \lfloor 2\sqrt{r} \log n \rfloor$, and $R_p := \mathbb{Z}/p[x]/(x^r - 1)$ then we have $(x+a)^n = x^n + a$ in R_n for $a = 1, \dots, l$. Let

$$I := \{m \in \mathbb{N} \mid (x+a)^m = x^m + a \text{ in } R_p \forall a = 1, \dots, l\}$$

then $1, p, n \in I$. We aim to show that I consists of the powers of p .

1.2 Lemma If $m, m' \in I$ then $mm' \in I$ (I is a multiplicative semigroup).

In R_p we have $(x+a)^{mm'} = (x^m + a)^{m'}$. On the other hand

$$(x+a)^{m'} - x^{m'} - a = (x^r - 1)u(x) \text{ in } \mathbb{Z}/p[x]$$

Replacing x with x^m yields

$$(x^m + a)^{m'} - x^{mm'} - a = (x^{mr} - 1)u(x) = (x^r - 1)(1 + x^r + \dots + x^{r(m-1)})u(x^m) = 0 \text{ in } R_p$$

So $(x^m + a)^{m'} = x^{mm'} + a$ in R_p and $mm' \in I$ ■

Define I_0 to be the group generated by p and n in $(\mathbb{Z}/r)^*$ and let $t = |I_0|$. Then $t \geq 4(\log n)^2$ since t was assumed to be the order of n in $(\mathbb{Z}/r)^*$.

1.3 Lemma If $1 \leq a_1, \dots, a_k \leq l$ and $f(x) = \prod_{i=1}^k (x + a_i) \in \mathbb{Z}/p[x]$

then $f(x)^m = f(x^m)$ in R_p for all $m \in I$.

We proceed via induction on k . The base case, $k = 1$, is clear from the definition of I . Now assume that $f_k(x) = f_{k-1}(x)(x + a_k)$ where the result holds for f_{k-1} . Then in R_p

$$f_k(x)^m = f_{k-1}(x)^m (x + a_k)^m = f_{k-1}(x^m) (x^m + a_k) = f_k(x^m)$$

■

For the next two Lemmas we introduce the following notation:

Let $h(x)$ be an irreducible factor of $\frac{x^r-1}{x-1}$ in $\mathbb{Z}/p[x]$, and ζ a root of h in $\overline{\mathbb{Z}/p}$.

Also let $F := \mathbb{Z}/p(\zeta) = \mathbb{Z}/p[x]/(h(x))$ be a finite field with $G := \langle \zeta + a \mid 1 \leq a \leq l \rangle \subseteq F^*$.

1.4 Lemma $|G| \geq \binom{t+l+1}{t-1}$

Let $f(x) = \prod_{i=1}^k (x + a_i)$, $g(x) = \prod_{i=1}^{k'} (x + b_i)$, $1 \leq a_i, b_i \leq l$; $k, k' \leq t-1$. We will show that $f(\zeta) \neq g(\zeta)$ in F so they yield distinct elements of G and so the size of G is bigger than the number of polynomials of the same form as f .

If $f(\zeta) = g(\zeta)$ then for all $m \in I_0$ we have

$$f(\zeta^m) \stackrel{1.3}{=} f(\zeta)^m = g(\zeta)^m \stackrel{1.3}{=} g(\zeta^m)$$

so the polynomial $f(x) - g(x)$ has roots ζ^m , $m \in I_0$ (since $\zeta^r = 1$, we are working mod r) and these are all distinct so $f - g$ has at least t roots. But $\deg(f - g) \leq \max(k, k') \leq t-1$ so $f(x) = g(x)$, thus distinct polynomials give distinct elements of G . ■

1.5 Lemma If n is not a power of p then $|G| \leq \frac{1}{2}n^{2\sqrt{t}}$

Let $J := \{n^i p^j \mid 0 \leq i, j \leq \lfloor \sqrt{t} \rfloor\} \subseteq I$ (recall 1.3). If n is not a power of p then all these terms are distinct and $|J| \geq (\lfloor \sqrt{t} \rfloor + 1)^2 > t$.

Now $\exists m, m' \in J$ with

$$m \equiv m' \pmod{r}$$

because the image of J in $(\mathbb{Z}/r)^*$ is contained in I_0 but $|I_0| = t < |J|$ so reduction mod r cannot be injective.

Again, let $f(x) = \prod_{i=1}^k (x + a_i)$, $1 \leq a_i \leq l$ and set $g = f(\zeta) \in G$. Then

$$g^m = f(\zeta)^m \stackrel{m \in J \subseteq I}{=} f(\zeta^m) \stackrel{m \equiv m' \pmod{r}, \zeta^r=1}{=} f(\zeta^{m'}) = f(\zeta)^{m'} = g^{m'}$$

so

$$G \subseteq \{ \text{roots of } x^m - x^{m'} \} \subseteq \bar{F}$$

and $|G| \leq \max(m, m') \leq (np)^{\sqrt{t}} \leq \frac{1}{2}n^{2\sqrt{t}}$. ■

Finally we return to the proof of the main theorem:

If n is not a power of p then by Lemma 1.5

$$|G| \leq \frac{1}{2}n^{2\sqrt{t}}$$

on the other hand Lemma 1.4 gives

$$|G| \geq \binom{t+l+1}{t-1}.$$

Recall $\sqrt{t} \geq 2 \log n \Rightarrow t \geq 2\sqrt{t} \log n$ and $l = \lfloor 2\sqrt{r} \log n \rfloor \geq 2\sqrt{t} \log n$ since $I_0 \leq (\mathbb{Z}/r)^*$, so

$$|G| \geq \binom{t+l+1}{t-1} \geq \binom{l+1 + \lfloor 2\sqrt{t} \log n \rfloor}{\lfloor 2\sqrt{t} \log n \rfloor} \geq \binom{\lfloor 4\sqrt{t} \log n \rfloor}{\lfloor 2\sqrt{t} \log n \rfloor} > \frac{1}{2} n^{2\sqrt{t}}$$

by Stirling's formula. Thus n is a prime power. ■

1.6 Conjecture *If r is an odd prime which does not divide the odd n and*

$$(x+1)^n = x^n + 1 \quad \text{in } R_n$$

then either n is prime or $n^2 \equiv 1 \pmod{r}$

This seems to be too strong according to the counter conjecture

1.7 Conjecture *For any prime $r \geq 5$ $\exists n$ such that $r \nmid n(n^2 - 1)$ and*

$$(x+1)^n = x^n + 1 \quad \text{in } R_n$$

What is the smallest n for a given r ? Denote it by $n_0(r)$. Now

$$(x+1)^n = x^n + 1 \text{ in } R_n \iff (x+1)^n \equiv x^n + 1 \pmod{x^r - 1} \text{ in } \mathbb{Z}/r[x]$$

If $r > n$ this implies

$$(x+1)^n = x^n + 1 \text{ in } \mathbb{Z}/n[x] \implies n \text{ is prime}$$

So $n_0(r) > r$. (numerical evidence shows $n_0(5)$ is large)

2 Notes from 2 Nov 2006: Sudan's Algorithm

Let x_1, x_2, \dots, x_n be distinct elements of the field F , and $t, d \geq 1$ integers.

Problem P Given $y_1, \dots, y_n \in F$, find all polynomials $f(x) \in F[x]$, $\deg f \leq d$ such that $f(x_i) = y_i$ for at least t values of i .

[cf Reed-Solomon codes]

Now if $f(x) \neq g(x)$ are polynomials of degree $\leq d$ then $\deg(f(x) - g(x)) \leq d$ so $f(x_i) = g(x_i)$ for at most d values of i .

When is there at most one solution?

2.1 Proposition *The Problem P has at most one solution $f(x) \in F[x]$ if $2t - n > d$.*

Consider $I, J \subseteq \{1, 2, \dots, n\}$ of size $\geq t$, then if

$$f(x_i) = y_i \text{ for } i \in I \quad g(x_i) = y_i \text{ for } i \in J$$

then $f(x_i) = g(x_i)$ for $i \in I \cap J$ so $f = g$ if $|I \cap J| > d$ but

$$|I \cap J| = |I| + |J| - |I \cup J| \geq 2t - |I \cup J| \geq 2t - n.$$

So if $2t - n > d$ the problem has at most one solution. ■

If $t = n$, that is we need all $f(x_i) = y_i$, and $n > d$ then we have at most one solution, and Lagrange interpolation using the first $d + 1$ elements

$$f(x) = \sum_{j=1}^{d+1} y_j \prod_{i=1, i \neq j}^{d+1} \frac{x - x_i}{x_j - x_i}$$

gives a candidate which can then be checked to see if $f(x_i) = y_i$ for the elements $i > d + 1$.

An approach to problem P when $t \geq d + 1$ would be to take every $I \subseteq \{1, 2, \dots, n\}$ with $|I| = d + 1$ and compute the unique f_I of degree $\leq d$ with $f(x_i) = y_i$ for $i \in I$ and then compute the $f_I(x_i)$ for $i \notin I$; keeping those f_I for which $f_I(x_i) = y_i$ for at least $t - (d + 1)$ values of $i \notin I$.

This process requires one to investigate $\binom{n}{d+1}$ polynomials.

There is an algorithm due to Berlekamp and Massey that when $2t - n > d$ either decides there is no solution or produces the unique solution efficiently (in finite fields).

2.2 Theorem *Sudan's algorithm solves problem P in polynomial time if $t > 2\sqrt{nd}$ and shows (by generating them) that there are at most $\sqrt{\frac{n}{d}}$ solutions in this case.*

We can summarize the different regimes as follows:

$$\begin{array}{lll}
 & & \text{e.g. } n = 16d \\
 t > \frac{n+d}{2} & \text{at most one solution} & t > 17d/2 \\
 t > 2\sqrt{nd} & \text{few solutions} & t > 8d, \text{ at most 3 solutions} \\
 & \vdots & \\
 t = d + 1 & \binom{n}{d+1} & \binom{16d}{d+1} \gg c^d \text{ solutions}
 \end{array}$$

The idea of Sudan's approach is

Construct a curve through all the points (x_i, y_i) , then a polynomial passing through many of the points will intersect this special curve numerous times and so by Bezout's theorem must share a common factor with this curve. The list of candidate polynomials will be constructed from the components of the curve.

Set $D = \lfloor \sqrt{nd} \rfloor$ and $l = \lfloor \sqrt{\frac{n}{d}} \rfloor$.

We want to construct $0 \neq Q(x, y) \in F[x, y]$ such that $Q(x_i, y_i) = 0$ for $i = 1, \dots, n$ and $\deg_x Q \leq D$ and $\deg_y Q \leq l$. Write

$$Q(x, y) = \sum_{i=0}^n \sum_{j=0}^l a_{ij} x^i y^j \quad \text{for some } a_{ij} \in F$$

then the conditions $Q(x_i, y_i) = 0$ for $i = 1, \dots, n$ give linear equations in the a_{ij} .

We have n equations in

$$(D + 1)(l + 1) > \sqrt{nd} \sqrt{\frac{n}{d}} = n$$

unknowns so a non-zero solution exists.

Suppose $f(x) \in F[x]$ has degree at most d and $f(x_i) = y_i$ for $i \in I \subseteq \{1, \dots, n\}$ with $|I| = t$. Then for $i \in I$

$$Q(x_i, f(x_i)) = Q(x_i, y_i) = 0$$

so $Q(x, f(x))$ has t zeros, and as a polynomial in x ,

$$\deg Q(x, f(x)) \leq D + ld \leq \sqrt{nd} + \sqrt{\frac{n}{d}} d = 2\sqrt{nd} \quad \underbrace{\leq t}_{\text{by hypothesis}}$$

so $Q(x, f(x))$ is identically zero.

This means that any solution $f(x)$ to problem P under these hypotheses satisfies $Q(x, f(x)) \equiv 0$

so $y - f(x) \mid Q(x, y)$ or

$$Q(x, y) = \prod_{k=1}^K \underbrace{(y - f_k(x))}_{\text{irred. in } F[x,y]} Q_1(x, y)$$

where the solutions to problem P must be one of the f_k .

Since $\deg_y Q \leq l$ we get $K \leq l \leq \sqrt{\frac{n}{d}}$.

To exhibit the solutions mentioned in the theorem we need to learn how to factor $Q(x, y)$ as a product of irreducibles.

2.3 Example Let $\mathbb{F}_4 = \{0, 1, \omega, 1 + \omega\}$, and set $d = 1$ so we want linear polynomials $f(x) = ax + b$, and $n = 5$ (the fifth value will be the slope [value at ∞]).

Suppose you are given y_1, \dots, y_5 ; construct Q as a quadratic with the fifth condition that the line $y = y_5x$ is asymptotic to $\{Q = 0\}$.

A conic has 6 coefficients to match the 5 conditions allowing one to determine 1 solution.

If

- Q is irreducible, there are no solutions.
- $Q = \text{constant} \cdot (y - f_1)^2$, there is one $f = f_1$
- $Q = \text{constant} \cdot (y - f_1)(y - f_2)$, there are two solutions $f = f_1, f_2$

As long as $t \geq 3$ then the solutions to P are factors of Q [A conic meets a line in at most 2 points unless the conic contains the line]