La criba de cuerpos de números.

En vez de trabajar sobre $\mathbb{Z}$ trabajamos sobre ~~est~~ anillos de "enteros" más grande que $\mathbb{Z}$. P. ej: $\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$

Es muy complicado y entonces miramos por arriba como es:

Queremos factorizar:

$2^{450} \approx N = pq$ $\quad p \neq q$

Buscamos $f(x) \in \mathbb{Z}[x]$ polinomio con coeficientes en $\mathbb{Z}$ de grado ~~chico~~ bajo. irreducible y mónico.

$m \in \mathbb{Z} \setminus \{0\}$ t.q. $f(m) \equiv 0 \pmod N$

$= 2^{\frac{512}{1}}$

Ej Si queremos factorizar $N = 2^9 + 1$, podríamos elegir

2^{103} y $f(x) = x^5 + 8$ porque

$$f(m) = f(2^{103}) = 2^{515} + 8$$

$$= 8(2^{512} + 1)$$

$$\equiv 0 \pmod{2^{512}+1}.$$

Sea $d = \deg(f)$ y $\beta (\in \mathbb{C})$ una raíz de f.

y trabajamos con el conjunto

$\mathbb{Z}[\beta]$

Ej $f(x) = 1 + 3x - 2x^3 + x^4$ β nc raíz

$$\mathbb{Z}[\beta] = \{ a_0 + a_1\beta + a_2\beta^2 + a_3\beta^3 : a_i \in \mathbb{Z} \}.$$

↓

por β^3 porque sabemos que

$$0 = 1 + 3\beta - 2\beta^3 + \beta^4$$

$$\Leftrightarrow \text{ o sea } \beta^4 = 2\beta^3 - 3\beta + 1 \quad (*)$$

y cada vez que tenemos un β^4 se puede cambiar por $2\beta^3 - 3\beta + 1$

$u, v \in \mathbb{Z}[\beta]$

$u+v$: coeficiente por coeficiente

$u \cdot v$: multiplicar como polinomios y reducir usando la relación $(*)$

Ej $u = 2 - 4\beta + 7\beta^2 + 3\beta^3$ $\quad v = 1 + 2\beta - 4\beta^2 - 2\beta^3$

$$u \cdot v = 2 - 9\beta^2 + 29\beta^3 - 14\beta^4 - 26\beta^5 - 6\beta^6$$

$$= 2 - 9\beta^2 + 29\beta^3 - 14(2\beta^3 - 3\beta + 1) - 26\beta^2(2\beta^3 - 3\beta + 1)$$

etc.

$\Leftrightarrow$ se puede dividir $u \cdot v$ por $\beta^4 + 2\beta^3 + 3\beta - 1$ como polinomios y guarde el resto

El siguiente paso es ~~entonces~~ encontrar muchos pares de enteros

$(a_1, b_1) \cdots (a_k, b_k)$

t.q $\prod_{i=1}^{k} (a_i - b_i m) = \square \in \mathbb{Z}$ $\quad \prod_{i=1}^{k} (a_i - b_i \beta) = \square \in \mathbb{Z}[\beta]$

$= A^2$ $\quad = \alpha^2$

Como $\alpha^2 \in \mathbb{Z}[\beta]$ & $\exists c_i \in \mathbb{Z}$ t.q

$$\alpha = c_0 + c_1 \beta + \cdots + c_{d-1} \beta^{d-1}$$

~~Como $f(m) \equiv 0 \pmod N$ si lo pensamos como~~

~~$a_0 + a_1 m + \cdots + a_{d-1} m^{k-1} \equiv 0 \pmod N$ en $\mathbb{Z}[\beta]$~~

~~y como $f(\beta) = 0$~~

~~$b_0 + b_1 \beta + \cdots + b_{d-1} \beta^{d-1} = 0$~~

~~$\equiv 0 \pmod N$~~ (donde reducimos los coef mód N)

Afirmación: Como $f(m) \equiv 0 \pmod N$ se puede probar que

$m \equiv \beta \pmod N$ en $\mathbb{Z}[\beta]$.

Entonces por un lado $A^2 \equiv \alpha^2 \pmod N$ en $\mathbb{Z}[\beta]$

por el otro $\alpha \equiv c_0 + c_1 m + \cdots + c_{d-1} m^{d-1} \pmod N$ en $\mathbb{Z}[\beta]$

Entonces

$$A^2 = (c_0 + c_1 m + \cdots + c_{d-1} m^{d-1})^2 \pmod N$$

y tenemos una congruencia $A^2 \equiv B^2 \pmod N$ en $\mathbb{Z}$. (no $\mathbb{Z}[\beta]$)

y unas veces, con alta probabilidad $\mathrm{mcd}(A-B, N)$ nos da un factor no trivial.

Como antes hay tres pasos

1 Encontrar relaciones. encontrar $a-bm$ "lisos"

2 Eliminar : algebra lineal

3 mcd

¿Qué quiere decir "liso"?

$a-b\beta$ "liso" en $\mathbb{Z}[\beta]$ hay varios problemas

1) $\mathbb{Z}[\beta]$ en general no tiene factorización única:

p.ej. en $\mathbb{Z}[\sqrt{-5}]$, $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$

Entonces en vez de factorizar números, factorizamos ideales

$a-b\beta$ es liso si los ideales en la factorización de $(a-b\beta)$ son pequeños.

2) El anillo $\mathbb{Z}[\beta]$ tal vez no tiene factorización única, pero hay un anillo $\mathcal{O}_F$ de $\mathbb{Q}(\beta)$ llamado el anillo de enteros del cuerpo de números $\mathbb{Q}(\beta)$ donde sí hay factorización única.

3) Supongamos que ~~llegamos~~ logramos a escribir el ideal

$\prod (a_i - b_i \beta)$ como el cuadrado de un ideal I en $\mathbb{Z}[\beta]$. Por ahí vez el ideal I no es generado por un ~~único~~ solo elemento y además si fuera

$I = (\gamma)^2$ sabemos solamente que

$\prod (a_i - b_i \beta) = u \gamma^2$ para algún $u \in \mathbb{Z}[\beta]^\times$

y en general hay infinitos $u \in \mathbb{Z}[\beta]^\times$.

<u>Def</u>: $(R, +, \cdot)$ anillo I es un ideal si ~~absorbe~~ es grupo aditivo que absorbe multiplicación por elementos de R:

1. $(I, +)$ subgrupo de $(R, +)$
2. $\forall x \in I, \forall r \in R \quad x \cdot r \in I$ y $r \cdot x \in I$.

<u>Ej</u>: $4\mathbb{Z}$ es un ideal en $\mathbb{Z}$. y es generado por 4

$(I, +) = \langle 4 \rangle : \{ 4+4, 4+4+4, 4-4, 4-4-4, \dots \}$

Mañana en el práctico hablarán un poco de esto.

Por hoy quiero hablar un poco del primer paso:

encontrar $m \in \mathbb{Z}$, polinomio món e irred. de grado pequeño

tq $f(m) \equiv 0 \pmod N$.

Primero: elegimos d. $\quad (N/\ell)^{1/d} \leq m \leq N^{1/d}$

Segundo: elegimos $m \in \mathbb{Z}$ tq

Tercero: escribir N en base m.

$$N = c_0 + c_1 m + c_2 m^2 + \cdots + c_{d-1} m^{d-1} + c_d m^d$$

La condición en $m \Rightarrow c_d = 1$ y entonces

$f(x) = c_0 + c_1 x + \cdots + c_d x^d$ es tiene m como raíz módulo N.

También pedimos que el polinomio sea irreducible: Si no lo fuera $f(x) = h(x) g(x)$

$\Rightarrow f(m) = g(m) h(m) \Rightarrow$ tenemos una factorización de m.

¿Por qué el NFS aunque es mucho más complicado que el QS?

Thm: Sea $0 < \varepsilon < 1$; $L_\varepsilon(x) = e^{(\ln x)^\varepsilon (\ln\ln x)^{1-\varepsilon}}$

Bajo condiciones razonables, el NFS toma $L_{1/3}(N)^c$

pasos para $c \leq 2$ (en general).

El QS es como $L_{1/2}(N)^c$, en esta notación.

Calculando logaritmos discretos en $\mathbb{F}_p$ usando el método de los cálculos de índices. (m1)

---

g raíz primitiva

Queremos resolver $g^x \equiv h \pmod p$.

- Elegimos B y resolvemos $g^x = \ell \pmod p$ $\forall$ primo $\ell \leq B$

  ★ o sea calculamos $\log_g(\ell)$ para cada primo $\ell \leq B$

- miramos los productos

  $h \cdot g^{-k} \pmod p$ $k = 1, 2, \dots$

  hasta encontrar k t.q. $h \cdot g^{-k} \pmod p$ es B-liso

$$h \cdot g^{-k} \equiv \prod_{\ell \leq B} \ell^{e_\ell} \pmod p$$

- concluimos

$$\log_g(h) \equiv k + \sum_{\ell \leq B} e_\ell \cdot \log_g(\ell) \pmod{p-1}$$

↑ porque $\mathbb{F}_p^*$ es módulo $p-1$ por Fermat

¿Cómo hacemos el paso ★?

Para potencias al azar calculamos $g_i \equiv g^i \pmod p$ con $0 < g_i < p$.

Si g_i no es B-liso los descartamos. Si g_i es B-liso,

$$g_i = \prod_{\ell \leq B} \ell^{u_\ell(i)}$$

$$\Rightarrow \quad i \equiv \log_g(g_i) = \sum_{\ell \leq B} u_\ell(i) \log_g(\ell) \pmod{p-1}$$

Se ve que las únicas incógnitas son los $\log_g(l)$. Si encontramos más que $\pi(B)$ tipo ecuaciones, como esta usando álgebra lineal (módulo l) se puede hallar una solución. Para hacer álgebra lineal mod $p-1$ usamos CRT.