UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

El Método ρ de Pollard

Alan Reyes-Figueroa

Teoría de Números

(Aula 23) 29.septiembre.2023

El Método ρ de Pollard

Suponga que n es un número compuesto muy grande. Usando un test de pseudoprimalidad, podemos mostrar que n es compuesto sin si quiera exhibir un divisor propio de n.

Calcular una factoración de n implica mucho más trabajo. Si p denota el menor factor primo de n, podemos localizar p luego de p pruebas. Como $p \leq \sqrt{n}$, esto requiere a lo sumo $\sqrt{n}$ operaciones.

Describimos a continuación un método para localizar el menor factor primo p de n con orden $O(\sqrt{p})$ operaciones.

Lema

Suponga $1 \leq k \leq n$, *y que los números* $u_1, u_2, \ldots, u_k$ *son elegidos de forma independiente dentro del conjunto* $\{1, 2, ldots, n\}$. *La probabilidad de que todos los* u_j *son distintos es*

$$\mathbb{P} = \left(1 - \tfrac{1}{n}\right)\left(1 - \tfrac{2}{n}\right) \ldots \left(1 - \tfrac{k-1}{n}\right).$$

El Método ρ de Pollard

Ejemplo: (Lema del Cumpleaños).
Como ejemplo, tomemos $n = 365$. y $k = 23$, la probabilidad en cuestión es menor a $\frac{1}{2}$. En otras palabras, cuando $k = 23$, la probabilidad de que al elegir al azar 23 personas, al menos 2 de ellas tengan el mismo día de cumpleaños es mayor a $\frac{1}{2}$.

En general, la probabilidad $\mathbb{P}$ anterior es aproximadamente $\mathbb{P} \approx exp(-\frac{k^2}{2n})$. Así, los u_j serán probablemente distintos para valores de k pequeños comparados con $\sqrt{n}$, pero probablemente no serán distintos para valores de k grandes comparados con $\sqrt{n}$.

Supongamos ahora que n es un entero positivo muy grande, cuyo menor divisor primo es p. Si elegimos $u_1, u_2, \ldots, u_k$, con $1 \leq u_j \leq n$, cuando k es grande comparado con $\sqrt{p}$, pero pequeño comparado con $\sqrt{n}$, entonces es muy probable que los u_j sean distintos $(\text{mod } m)$, pero probablemente no serán distintos $(\text{mod } p)$.

Así, existirán índices i, j, $1 \leq i < j \leq k$, tales que $1 < (u_i - u_j, n) < n$.

El Método ρ de Pollard

Testar todos los pares (i, j), $1 \leq i < j \leq k$, es algo sencillo mediante el Algoritmo de Euclides. Pero son en total $\binom{k}{2}$ pares.

Para simplificar el trabajo, adoptamos el siguiente esquema: generamos los u_j mediante alguna recursión de la forma

$$u_{j+1} = f(u_j),$$

donde $f \in \mathbb{Z}[x]$ es un polinomio con coeficientes enteros.

El proceso de elegir $f(u)$ no es importante, basta con que sea un polinomio fácil de calcular, y que sea un polinomio de grado $\deg(f) \geq 2$. (En general, polinomios lineales no se desempeñan bien).

Por ejemplo, $f(u) = u^2 + 1$ es una buena elección.

La ventaja de generar los u_j de esta manera es que si $u_i \equiv u_j \pmod{d}$, entones

$$u_{i+1} = f(u_i) \equiv f(u_j) = u_{j+1} \pmod{d}.$$

El Método ρ de Pollard

Luego, la secuencia u_j se hace periódica $\pmod d$, con período $j - i$.

En otras palabras, si hacemos $r = j - i$ entonces

$$u_s \equiv u_t \pmod d, \quad \text{siempre que} \quad s \equiv t \pmod r,\ s, t \geq i$$

En particular, tomando $t = 2s$, entonces $u_s \equiv u_{2s} \pmod d$.

Así, entre los números $u_{2s} - u_s$, deberíamos esperar uno que satisfaga

$$1 < d = (u_{2s} - u_s, n) < n,$$

produciendo automáticamente un divisor no trivial de n. El método requiere alrededor $s \approx O(\sqrt{p})$ intentos.

Definición

*El anterior es llamado el **algoritmo** o **método** ρ **de Pollard**.*

Ejemplo

Usamos el método ρ de Pollard para hallar un divisor propio de $n = 36287$. Tomemos $f(u) = u^2 + 1$ y sea $u_0 = 1$. Entonces, si $u_{i+1} \equiv f(u_i) \pmod{n}$

i	1	2	3	4	5	6	7
u_i	2	5	26	677	22886	2439	33941
i	8	9	10	11	12	13	14
u_i	24380	3341	22173	25652	26685	29425	22806

Luego:

i	$2i$	u_{2i}	u_i	$u_{2i} - u_i$	$(u_{2i} - u_i, n)$
1	2	5	2	3	$(3, n) = 1$
2	4	677	5	672	$(672, n) = 1$
3	6	2439	26	2413	$(2413, n) = 1$
4	8	24380	677	23703	$(23703, n) = 1$
5	10	22173	22886	713	$(713, n) = 1$
6	12	26685	2439	24246	$(24246, n) = 1$
7	14	22806	33941	11135	$(11135, n) = 131$

Ejemplo

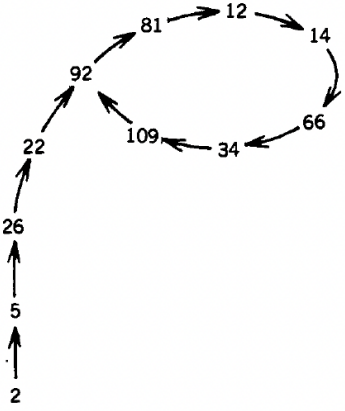

Diagrama del método ρ de Pollard.