Bab 11

Matematika IV - Kuadrat

Di bab ini kita akan bahas konsep *quadratic residue* dan akar kuadrat modulo bilangan ganjil.

11.1 Quadratic Residue

Kita akan bahas *quadratic residue* yang kerap digunakan dalam test bilangan prima dan dalam beberapa teknik penguraian. Akan tetapi, sebelum kita bahas *quadratic residue*, kita perkenalkan dahulu konsep akar dari 1 (*root of unity*), yaitu solusi persamaan $x^n = 1$ dalam suatu *finite field*, dan konsep akar primitif (*primitive root*) , yaitu akar yang jika dipangkatkan mengunjungi semua akar-akar persamaan yang sama dalam suatu *finite field*, dengan kata lain, semua akar-akar persamaan merupakan pemangkatan dari *primitive root*.

Definisi 25 (Root of Unity) *Untuk suatu finite field* $\mathbf{F}$*:*

- *elemen* a *adalah* n*-th root of unity jika* $a^n = 1$ *dalam* $\mathbf{F}$*;*
- *elemen* a *adalah primitive* n*-th root of unity jika* $a^n = 1$ *dalam* $\mathbf{F}$ *dan untuk setiap elemen* b *dengan* $b^n = 1$ *terdapat suatu* j *dimana* $b = a^j$ *dalam* $\mathbf{F}$*.*

Contoh dari *primitive root* adalah *generator* g untuk $\mathbf{F}_q^*$ dimana g merupakan akar dari persamaan $x^{\phi(q)} = 1$ dalam $\mathbf{F}_q$ dan setiap akar dari persamaan (jadi setiap elemen dari $\mathbf{F}_q^*$) merupakan pemangkatan dari g. Teorema berikut menjawab pertanyaan ada berapa solusi persamaan $x^n = 1$ dalam suatu *finite field* $\mathbf{F}_q$ (banyaknya *n-th root of unity*).

Teorema 53 *Jika* g *adalah generator untuk* $\mathbf{F}_q^*$*, maka* g^j *merupakan* n*-th root of unity (solusi persamaan* $x^n = 1$*) jika dan hanya jika* $nj \equiv 0 \pmod{\phi(q)}$*.*

Banyaknya n-th root of unity adalah $\gcd(n, \phi(q))$ *dan* $\mathbf{F}_q$ *mempunyai primitive n-th root of unity jika dan hanya jika* $n|\phi(q)$. *Jika* ξ *merupakan primitive n-th root of unity maka* ξ^j *juga merupakan primitive n-th root of unity jika dan hanya jika* $\gcd(j, n) = 1$.

Mari kita buktikan teorema 53. Setiap elemen dari $\mathbf{F}_q^*$ merupakan pemangkatan g^j dari *generator* g, dan pemangkatan g^{nj} menghasilkan 1 jika dan hanya jika $\phi(q)$ membagi nj. Jadi elemen g^j merupakan *n-th root of unity* jika dan hanya jika $nj \equiv 0 \pmod{\phi(q)}$. Untuk menunjukkan bahwa banyaknya *n-th root of unity* adalah $d = \gcd(n, \phi(q))$, kita fokus pada persamaan $nj \equiv 0 \pmod{\phi(q)}$ yang mempunyai bentuk dasar

$$ax \equiv b \pmod{n}. \tag{11.1}$$

Jika $d = \gcd(a, n)$, maka persamaan 11.1 mempunyai solusi untuk x jika dan hanya jika $d|b$, dan solusi persamaan 11.1 sama dengan solusi untuk

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}. \tag{11.2}$$

Karena $\gcd(\frac{a}{d}, \frac{n}{d}) = 1$, maka $\frac{a}{d}$ mempunyai *inverse* dalam $\mathbf{Z}/\frac{n}{d}\mathbf{Z}$, dan solusi untuk x didapat dengan mengalikan bagian kiri dan kanan persamaan 11.2 dengan *inverse* tersebut. Kembali pada banyaknya *n-th root of unity*, karena $d|0$, maka kita dapat fokus pada persamaan

$$\frac{n}{d}j \equiv 0 \pmod{\frac{\phi(q)}{d}}$$

yang, karena $\gcd(\frac{n}{d}, \frac{\phi(q)}{d}) = 1$, ekuivalen dengan

$$j \equiv 0 \pmod{\frac{\phi(q)}{d}}$$

yang berarti j harus merupakan kelipatan dari $\frac{\phi(q)}{d}$. Ada d kelipatan $\frac{\phi(q)}{d}$ $\pmod{\phi(q)}$ yaitu

$$\begin{aligned}
j &\equiv \frac{0\phi(q)}{d} \pmod{\phi(q)} \\
j &\equiv \frac{1(\phi(q))}{d} \pmod{\phi(q)} \\
j &\equiv \frac{2(\phi(q))}{d} \pmod{\phi(q)} \\
&\cdots \\
j &\equiv \frac{(d-1)(\phi(q))}{d} \pmod{\phi(q)}.
\end{aligned}$$

$\mathbf{F}_q$ mempunyai *primitive n-th root of unity* jika dan hanya jika banyaknya *n-th root of unity* adalah n, jadi $d = n$ yang berarti $n|\phi(q)$. Sekarang kita buktikan bagian terahir teorema 53. Jika $n|\phi(q)$ maka $\mathbf{F}_q$ mempunyai *primitive n-th root of unity*, satu diantaranya adalah $\xi = g^{\phi(q)/n}$. Pemangkatan $\xi^i = 1$ jika dan hanya jika $n|i$. Pemangkatan $(\xi^j)^k = 1$ jika dan hanya jika

$$kj \equiv 0 \pmod{n}. \tag{11.3}$$

Jadi ξ^j mempunyai *order* n (persamaan 11.3 tidak berlaku untuk $0 < k < n$) jika dan hanya jika $\gcd(j, n) = 1$, yang juga berarti terdapat $\phi(n)$ *primitive n-th root of unity* untuk $\mathbf{F}_q$. Selesailah pembuktian teorema 53. *Generator* g untuk suatu *cyclic group* G merupakan contoh dari *primitive root*: g merupakan solusi untuk $x^n = 1$ dimana n merupakan banyaknya elemen dalam G, dan untuk setiap elemen a dalam G (a juga merupakan solusi untuk $x^n = 1$), terdapat i dengan $0 \leq i < n$ dimana $a = g^i$.

Sekarang mari kita bahas konsep *quadratic residues*. Jika p merupakan suatu bilangan prima ganjil ($p > 2$), kita kerap ingin mengetahui elemen-elemen mana dari $\{1, 2, 3, \ldots, p-1\}$ ($\mathbf{F}_p^*$) yang merupakan kuadrat. Jika $a \in \mathbf{F}_p^*$ merupakan suatu kuadrat (misalnya $b^2 = a$), maka a memiliki tidak lebih dan tidak kurang dari dua akar pangkat dua yaitu $\pm b$ (karena persamaan $x^2 - a$ mempunyai paling banyak 2 solusi dalam suatu *field*, dan jika p ganjil maka b dan $-b$ merupakan dua solusi untuk x yang berbeda). Jadi semua kuadrat dalam $\mathbf{F}_p^*$ dapat dicari dengan mengkalkulasi b^2 untuk

$$b = 1, 2, 3, \ldots, (p-1)/2$$

karena setiap dari sisa bilangan sampai dengan $p - 1$ merupakan $-b$ untuk suatu b diatas. Jadi setengah dari bilangan dalam $\mathbf{F}_p^*$ merupakan kuadrat. Sebagai contoh, untuk $\mathbf{F}_{11}$ mereka adalah $1^2 = (-1)^2 = 1$, $2^2 = (-2)^2 = 4$, $3^2 = (-3)^2 = 9$, $4^2 = (-4)^2 = 5$ dan $5^2 = (-5)^2 = 3$. Kuadrat dalam $\mathbf{F}_p^*$ dinamakan *quadratic residues* sedangkan elemen-elemen yang bukan kuadrat disebut *non-residues*. Untuk $\mathbf{F}_{11}$ *non-residues* adalah 2, 6, 7, 8 dan 10.

Jika g merupakan *generator* untuk $\mathbf{F}_p^*$, setiap kuadrat merupakan g^j untuk suatu bilangan genap j. Sebaliknya setiap g^j, dengan j suatu bilangan genap, merupakan suatu kuadrat yaitu kuadrat dari $\pm g^{j/2}$.

Sekarang kita definisikan simbol Legendre (*Legendre symbol* dengan notasi $(\frac{a}{p})$) sebagai berikut:

Definisi 26 (Legendre Symbol)

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \textit{jika } p|a; \\ 1 & \textit{jika } a \textit{ merupakan quadratic residue} \pmod{p}; \\ -1 & \textit{jika } a \textit{ merupakan nonresidue} \pmod{p}. \end{cases}$$

Jadi $(\frac{a}{p})$ dapat digunakan untuk memberi indikasi apakah suatu bilangan bulat merupakan suatu *quadratic residue* $\pmod p$. Berikut adalah teorema penting mengenai simbol Legendre.

Teorema 54

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p.$$

Mari kita buktikan teorema 54. Jika $p|a$ maka kedua sisi dari persamaan akan sama dengan 0. Jika $p \not| a$ maka berdasarkan *Fermat's little theorem* (teorema 30) kita dapatkan

$$\begin{aligned} (a^{(p-1)/2})^2 &= a^{p-1} \\ &\equiv 1 \pmod p, \end{aligned}$$

jadi $a^{(p-1)/2} = \pm 1$. Jika g adalah suatu *generator* untuk $\mathbf{F}_p^*$ maka terdapat bilangan j dimana $a = g^j$. Kita ketahui bahwa a merupakan *quadratic residue* jika dan hanya jika j genap. Juga $a^{(p-1)/2} = g^{j(p-1)/2} = 1$ jika dan hanya jika $j(p-1)/2$ dapat dibagi oleh $(p-1)$ (karena *generator* menghasilkan 1 jika dan hanya jika dipangkatkan oleh kelipatan $(p-1)$). Jadi $j(p-1)/2$ dapat dibagi oleh $(p-1)$ jika dan hanya jika j dapat dapat dibagi 2 (j genap). Alhasil kedua sisi dari persamaan dalam teorema sama dengan 1 jika dan hanya jika j genap. Karena untuk $p \not| a$ kedua sisi persamaan menghasilkan ± 1 dan kedua sisi menghasilkan 1 jika dan hanya jika j genap, berarti kedua sisi menghasilkan -1 jika dan hanya jika j tidak genap (ganjil), jadi kedua sisi selalu sama, jadi selesailah pembuktian teorema 54. Berikut kita buktikan dahulu beberapa persamaan mengenai simbol Legendre sebelum kita bahas teorema mengenai *quadratic reciprocity*.

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right); \tag{11.4}$$

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \text{ jika } a \equiv b \pmod p; \tag{11.5}$$

$$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right) \text{ jika } \gcd(b,p) = 1; \tag{11.6}$$

$$\left(\frac{1}{p}\right) = 1; \tag{11.7}$$

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \tag{11.8}$$

$$\left(\frac{2}{n}\right) = (-1)^{(p^2-1)/8}. \tag{11.9}$$

Untuk membuktikan persamaan 11.4, kita gunakan teorema 54:

$$\begin{aligned}\left(\frac{ab}{p}\right) &\equiv (ab)^{(p-1)/2} \pmod p\\ &= a^{(p-1)/2}b^{(p-1)/2}\\ &\equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p.\end{aligned}$$

Untuk membuktikan persamaan 11.5, kita gunakan definisi *quadratic residue*: jika $a \equiv b \pmod p$, maka a merupakan *quadratic residue* $\pmod p$ jika dan hanya jika b merupakan *quadratic residue* $\pmod p$. Untuk membuktikan persamaan 11.6, kita gunakan persamaan 11.4:

$$\begin{aligned}\left(\frac{ab^2}{p}\right) &= \left(\frac{a}{p}\right)\left(\frac{b^2}{p}\right)\\ &= \left(\frac{a}{p}\right), \text{ jika } \gcd(b,p) = 1,\end{aligned}$$

karena $\left(\frac{b^2}{p}\right) = 1$ jika $\gcd(b,p) = 1$. Persamaan 11.7 didapat karena $1^2 = 1$ dan persamaan 11.8 didapat dari teorema 54 dengan $a = -1$. Sebelum membuktikan persamaan 11.9, kita buktikan dahulu teorema yang kita beri nama *Gauss's Lemma 1*. Untuk itu kita jelaskan notasi yang digunakan. Jika p adalah bilangan prima, maka kita dapat mempartisi $(\mathbf{Z}/p\mathbf{Z})^*$ menjadi dua subset:

$$\begin{aligned}P &= \{1,2,3,\ldots,(p-1)/2\} \subset (\mathbf{Z}/p\mathbf{Z})^*,\\ N &= \{-1,-2,-3,\ldots,-(p-1)/2\} \subset (\mathbf{Z}/p\mathbf{Z})^*.\end{aligned}$$

Untuk setiap $a \in (\mathbf{Z}/p\mathbf{Z})^*$, kita definisikan:

$$\begin{aligned}aP &= \{ax|x \in P\}\\ &= \{a, 2a, 3a, \ldots, (p-1)a/2\}.\end{aligned}$$

Sebagai contoh, $-1P = N$.

Teorema 55 (Gauss's Lemma 1) *Jika p adalah bilangan prima ganjil, dan $a \in (\mathbf{Z}/p\mathbf{Z})^*$, maka*

$$\left(\frac{a}{p}\right) = (-1)^{\mu}$$

dimana $\mu = |aP \cap N|$.

Pangkat μ sama dengan banyaknya elemen dari aP yang juga berada dalam N ("negatif"). Mari kita buktikan teorema 55. Jika $x, y \in P$ dan $x \neq y$, maka

$ax \neq \pm ay$ dalam $(\mathbf{Z}/p\mathbf{Z})^*$ (karena jika $ax \equiv \pm ay \pmod p$, maka $p|a(x \mp y)$, jadi $p|(x \mp y)$, sesuatu yang tidak mungkin karena x dan y adalah elemen yang berbeda dalam $\{1, 2, 3, \ldots, (p-1)/2\}$). Jadi elemen-elemen dari aP tersebar di himpunan-himpunan berikut:

$$\{\pm 1\}, \{\pm 2\}, \ldots \{\pm (p-1)/2\}$$

dimana dua elemen dari aP tidak mungkin berada dalam satu himpunan. Karena terdapat $(p-1)/2$ himpunan dan terdapat $(p-1)/2$ elemen dalam aP, maka setiap himpunan mempunyai satu elemen dari aP, tidak lebih dan tidak kurang. Jadi

$$aP = \{\varepsilon_i i | i = 1, 2, \ldots, (p-1)/2\}$$

dimana $\varepsilon_i = 1$ jika $\varepsilon_i i \in P$ dan $\varepsilon_i = -1$ jika $\varepsilon_i i \in N$. Kita kalikan semua elemen aP dalam $(\mathbf{Z}/p\mathbf{Z})^*$ menggunakan definisi pertama aP mendapatkan:

$$a^{(p-1)/2} \cdot ((p-1)/2)!.$$

Kita juga dapat menggunakan definisi alternatif untuk mendapatkan

$$(\prod_{i=1}^{(p-1)/2} \varepsilon_i) \cdot ((p-1)/2)!.$$

Jadi

$$\begin{aligned} a^{(p-1)/2} \cdot ((p-1)/2)! &= (\prod_{i=1}^{(p-1)/2} \varepsilon_i) \cdot ((p-1)/2)! \\ &= (-1)^\mu \cdot ((p-1)/2)! \end{aligned}$$

dalam $(\mathbf{Z}/p\mathbf{Z})^*$, dimana $\mu = |aP \cap N|$. Jadi

$$a^{(p-1)/2} \equiv (-1)^\mu \pmod p.$$

Dengan menggunakan teorema 54 kita dapatkan

$$\left(\frac{a}{p}\right) \equiv (-1)^\mu \pmod p$$

membuktikan teorema 55. Sekarang kita gunakan teorema 55 untuk membuktikan persamaan 11.9. Dengan $a = 2$, kita dapatkan

$$\begin{aligned} aP &= 2P \\ &= \{2, 4, 6, \ldots, p-1\}. \end{aligned}$$

Untuk $p \equiv 1 \pmod 4$,

$$2P = \{2, 4, \ldots, (p-1)/2, (p+3)/2, \ldots, p-1\}$$

dimana $(p-1)/4$ elemen pertama $\{2, 4, \ldots, (p-1)/2$ berada dalam P, dan sisanya $(p-1)/4$ elemen $\{(p+3)/2, \ldots, (p-1)\}$ berada dalam N. Jadi $\mu = |2P \cap N| = (p-1)/4$, dan menurut teorema 55:

$$\begin{aligned}\left(\frac{2}{p}\right) &= (-1)^{(p-1)/4} \\ &= ((-1)^{(p-1)/4})^{(p+1)/2} \\ &= (-1)^{(p^2-1)/8}.\end{aligned}$$

Perhatikan bahwa kita telah menggunakan fakta bahwa $(p+1)/2$ adalah bilangan ganjil, jadi $(\pm 1)^{(p+1)/2} = (\pm 1)$. Untuk $p \equiv -1 \pmod 4$,

$$2P = \{2, 4, \ldots, (p-3)/2, (p+1)/2, \ldots, p-1\}$$

dimana $(p-3)/4$ elemen pertama $\{2, 4, \ldots, (p-3)/2$ berada dalam P, dan sisanya $(p+1)/4$ elemen $\{(p+1)/2, \ldots, (p-1)\}$ berada dalam N. Jadi $\mu = |2P \cap N| = (p+1)/4$, dan menurut teorema 55:

$$\begin{aligned}\left(\frac{2}{p}\right) &= (-1)^{(p+1)/4} \\ &= ((-1)^{(p+1)/4})^{(p-1)/2} \\ &= (-1)^{(p^2-1)/8}.\end{aligned}$$

Perhatikan bahwa kita telah menggunakan fakta bahwa $(p-1)/2$ adalah bilangan ganjil, jadi $(\pm 1)^{(p-1)/2} = (\pm 1)$. Kita telah membuktikan persamaan 11.9 untuk $p \equiv 1 \pmod 4$ dan $p \equiv -1 \pmod 4$. Karena untuk bilangan prima ganjil p, $p \equiv \pm 1 \pmod 4$, maka selesailah pembuktian persamaan 11.9.

Teorema 56 (Quadratic Reciprocity) *Untuk dua bilangan prima ganjil p dan q:*

$$\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{q}{p}\right) & \textit{jika } p \equiv q \equiv 3 \pmod 4; \\ \left(\frac{q}{p}\right) & \textit{jika tidak.}\end{cases}$$

Untuk membuktikan teorema 56, kita bentuk *finite field* $\mathbf{F}_{p^{q-1}}$ (perhatikan bahwa $p^{q-1} \equiv 1 \pmod q$). Karena $q | p^{q-1} - 1$, maka menurut teorema 53, terdapat *primitive qth-root of unity* dalam $\mathbf{F}_{p^{q-1}}$ yang kita beri notasi ξ. Kita definisikan *Gauss sum* G:

$$G = \sum_{j=0}^{q-1} \left(\frac{j}{q}\right) \xi^j.$$

Kita ingin tunjukkan bahwa

$$G^2 = (-1)^{(q-1)/2} q. \tag{11.10}$$

Perhatikan bahwa

$$\sum_{j=0}^{q-1} \left(\frac{j}{q}\right) \xi^j \quad = \quad \sum_{j=1}^{q-1} \left(\frac{j}{q}\right) \xi^j,$$

karena $\left(\frac{0}{q}\right) = 0$, dan

$$\sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \xi^k \quad = \quad \sum_{k=1}^{q-1} \left(\frac{-k}{q}\right) \xi^{-k},$$

karena mengganti k dengan $-k$ dalam penjumlahan tetap menjumlahkan semua suku yang sama (setiap elemen $\neq 0$ dari *finite field* dikunjungi), jadi

$$\begin{aligned}
G^2 &= \sum_{j,k=1}^{q-1} \left(\frac{j}{q}\right) \xi^j \left(\frac{-k}{q}\right) \xi^{-k} \\
&= \left(\frac{-1}{q}\right) \sum_{j=1}^{q-1} \sum_{k=1}^{q-1} \left(\frac{jk}{q}\right) \xi^{j-k} \\
&= (-1)^{(q-1)/2} \sum_{j=1}^{q-1} \sum_{k=1}^{q-1} \left(\frac{jk}{q}\right) \xi^{j-k} \text{ (menggunakan 11.8)} \\
&= (-1)^{(q-1)/2} \sum_{j=1}^{q-1} \sum_{k=1}^{q-1} \left(\frac{j^2 k}{q}\right) \xi^{j-kj} \text{ (tukar } k \text{ dengan } kj) \\
&= (-1)^{(q-1)/2} \sum_{j=1}^{q-1} \sum_{k=1}^{q-1} \left(\frac{j^2 k}{q}\right) \xi^{j(1-k)} \\
&= (-1)^{(q-1)/2} \sum_{j=1}^{q-1} \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \xi^{j(1-k)} \text{ (menggunakan 11.6)} \\
&= (-1)^{(q-1)/2} \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \sum_{j=1}^{q-1} \xi^{j(1-k)} \\
&= (-1)^{(q-1)/2} \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \sum_{j=0}^{q-1} \xi^{j(1-k)} \\
&= (-1)^{(q-1)/2} \left(\frac{1}{q}\right) \sum_{j=0}^{q-1} \xi^{j(1-1)} \text{ (hanya } k = 1 \text{ yang memberi kontribusi)}
\end{aligned}$$

$$= \quad (-1)^{(q-1)/2}q.$$

Pada langkah ketiga dari ahir, penjumlahan dengan indeks j dapat dimulai dari 0 karena hanya menambahkan

$$\sum_{k=1}^{q-1}\left(\frac{k}{q}\right) = 0$$

(banyaknya *residue* dan *non-residue* sama $\pmod{q}$). Pada langkah kedua dari ahir, hanya penjumlahan dengan $k = 1$ yang dihitung, karena untuk $k \neq 1$ penjumlahan terdalam $(\sum_j)$ menghasilkan 0. Ini karena jika $k \neq 1$ maka ξ^{1-k} merupakan *non-trivial qth root of unity*, jadi jika setiap elemen dalam urutan

$$(\xi^{1-k})^0, (\xi^{1-k})^1, (\xi^{1-k})^2, \ldots, (\xi^{1-k})^{q-1}$$

dikalikan dengan ξ^{1-k} maka kita dapatkan elemen-elemen yang sama dengan urutan yang berbeda. Jadi

$$\xi^{1-k}\sum_{j=0}^{q-1}\xi^{(1-k)j} = \sum_{j=0}^{q-1}\xi^{(1-k)j}$$

dan

$$(\xi^{1-k} - 1)\sum_{j=0}^{q-1}\xi^{(1-k)j} = 0.$$

Karena $(\xi^{1-k} - 1) \neq 0$, maka

$$\sum_{j=0}^{q-1}\xi^{(1-k)j} = 0.$$

Kembali ke pembuktian teorema 56, kita dapatkan

$$\begin{aligned}
G^p &= (G^2)^{(p-1)/2}G \\
&= ((-1)^{(q-1)/2}q)^{(p-1)/2}G \\
&= (-1)^{(p-1)(q-1)/4}q^{(p-1)/2}G \\
&= (-1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right)G
\end{aligned}$$

menggunakan teorema 54 dengan $a = q$. Dengan menggunakan definisi dari G, kita juga dapatkan

$$G^p = (\sum_{j=0}^{q-1}\left(\frac{j}{q}\right)\xi^j)^p$$

$$\begin{aligned}
&= \sum_{j=0}^{q-1} \left(\frac{j}{q}\right) \xi^{jp} \\
&= \sum_{j=0}^{q-1} \left(\frac{p}{q}\right) \left(\frac{jp}{q}\right) \xi^{jp} \\
&= \left(\frac{p}{q}\right) \sum_{j=0}^{q-1} (jpq)\, \xi^{jp} \\
&= \left(\frac{p}{q}\right) G.
\end{aligned}$$

Menggunakan hasil sebelumnya untuk G^p, kita dapatkan

$$\left(\frac{p}{q}\right) G = (-1)^{(p-1)(q-1)/4} \left(\frac{q}{p}\right) G$$

dan dengan membagi kedua sisi dengan G kita dapatkan

$$\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{q}{p}\right).$$

Selesailah pembuktian teorema 56.

Simbol Legendre dapat digunakan hanya jika modulus adalah bilangan prima. Jika modulus belum tentu bilangan prima, kita harus menggunakan simbol Jacobi (*Jacobi symbol*).

Definisi 27 (Jacobi Symbol) *Jika*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$$

adalah prime factorization (unique factorization) dari n, maka simbol Jacobi didefinisikan sebagai berikut:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \dots \left(\frac{a}{p_m}\right)^{\alpha_m}.$$

Berikut adalah beberapa persamaan mengenai simbol Jacobi, dimana m, n adalah bilangan ganjil positif, dan a, b adalah bilangan bulat.

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right); \tag{11.11}$$

$$\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right); \tag{11.12}$$

$$\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right) \text{ jika } a \equiv b \pmod{n}; \tag{11.13}$$

$$\begin{aligned}
\left(\frac{-1}{n}\right) &= (-1)^{(n-1)/2}; && (11.14)\\
\left(\frac{2}{n}\right) &= (-1)^{(n^2-1)/8}; && (11.15)\\
\left(\frac{a}{n}\right)\left(\frac{n}{a}\right) &= (-1)^{\frac{a-1}{2}\frac{n-1}{2}} \text{ jika } \gcd(a,n)=1, a>0, a \text{ ganjil.} && (11.16)
\end{aligned}$$

Persamaan 11.11 dapat dijelaskan menggunakan definisi simbol Jacobi dan persamaan 11.4 mengenai simbol Legendre:

$$\begin{aligned}
\left(\frac{ab}{n}\right) &= \left(\frac{ab}{p_1}\right)^{\alpha_1} \cdots \left(\frac{ab}{p_m}\right)^{\alpha_m}\\
&= \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{b}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_m}\right)^{\alpha_m} \left(\frac{b}{p_m}\right)^{\alpha_m}\\
&= \left(\frac{a}{n}\right)\left(\frac{b}{n}\right).
\end{aligned}$$

Persamaan 11.12 didapat dari definisi simbol Jacobi:

$$\begin{aligned}
\left(\frac{a}{mn}\right) &= \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_j}\right)^{\alpha_j} \left(\frac{a}{q_1}\right)^{\beta_1} \cdots \left(\frac{a}{q_k}\right)^{\beta_k}\\
&= \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)
\end{aligned}$$

dimana

$$\begin{aligned}
m &= p_1^{\alpha_1} \ldots p_j^{\alpha_j} \text{ dan}\\
n &= q_1^{\beta_1} \ldots q_k^{\beta_k}.
\end{aligned}$$

Persamaan 11.13 dapat dijelaskan menggunakan definisi simbol Jacobi dan persamaan 11.5 mengenai simbol Legendre:

$$\begin{aligned}
\left(\frac{a}{n}\right) &= \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_m}\right)^{\alpha_m}\\
&= \left(\frac{b}{p_1}\right)^{\alpha_1} \cdots \left(\frac{b}{p_m}\right)^{\alpha_m}\\
&= \left(\frac{b}{n}\right)
\end{aligned}$$

dimana

$$n = p_1^{\alpha_1} \ldots p_m^{\alpha_m}.$$

Untuk membuktikan persamaan 11.14, kita tunjukkan dahulu untuk m, n bilangan ganjil,

$$\frac{m-1}{2} + \frac{n-1}{2} \equiv \frac{mn-1}{2} \pmod 2.$$

Karena m, n ganjil, maka terdapat m', n' dimana $m = 2m' + 1, n = 2n' + 1$, jadi

$$\begin{aligned} \frac{m-1}{2} + \frac{n-1}{2} &= \frac{2m'+1-1}{2} + \frac{2n'+1-1}{2} \\ &= m' + n'. \end{aligned}$$

Kita juga dapatkan

$$\begin{aligned} \frac{mn-1}{2} &= \frac{(2m'+1)(2n'+1)-1}{2} \\ &= \frac{4m'n' + 2m' + 2n' + 1 - 1}{2} \\ &= 2m'n' + m' + n'. \end{aligned}$$

Karena $m' + n' \equiv 2m'n' + m' + n' \pmod 2$, maka kita dapatkan

$$\frac{m-1}{2} + \frac{n-1}{2} \equiv \frac{mn-1}{2} \pmod 2.$$

Karena produk bilangan ganjil juga ganjil, maka kita dapatkan

$$\frac{n_1-1}{2} + \ldots + \frac{n_m-1}{2} \equiv \frac{n_1 \ldots n_m - 1}{2} \pmod 2.$$

Kembali ke persamaan 11.14:

$$\begin{aligned} \left(\frac{-1}{n}\right) &= \left(\frac{-1}{p_1}\right)^{\alpha_1} \ldots \left(\frac{-1}{p_m}\right)^{\alpha_m} \\ &= ((-1)^{(p_1-1)/2})^{\alpha_1} \ldots ((-1)^{(p_m-1)/2})^{\alpha_m} \\ &= ((-1)^{\alpha_1(p_1-1)/2}) \ldots ((-1)^{\alpha_m(p_m-1)/2}) \\ &= (-1)^k \end{aligned}$$

dengan $k = \sum_{i=1}^{k} \alpha_i(p_i - 1)/2$, jadi

$$\begin{aligned} k &= \underbrace{(p_1-1)/2 + \ldots + (p_1-1)/2}_{\alpha_1 \times} + \ldots + \underbrace{(p_m-1)/2 + \ldots + (p_m-1)/2}_{\alpha_m \times} \\ &\equiv (\underbrace{p_1 \ldots p_1}_{\alpha_1 \times} \ldots \underbrace{p_m \ldots p_m}_{\alpha_m \times} - 1)/2 \pmod 2 \\ &\equiv (p_1^{\alpha_1} \ldots p_m^{\alpha_m} - 1)/2 \pmod 2 \\ &\equiv (n-1)/2 \pmod 2. \end{aligned}$$

Jadi karena $(-1)^k = (-1)^{(n-1)/2}$, kita dapatkan

$$\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}.$$

Untuk membuktikan persamaan 11.15, kita tunjukkan dahulu untuk m, n bilangan ganjil,

$$\frac{m^2-1}{8} + \frac{n^2-1}{8} \equiv \frac{m^2n^2-1}{8} \pmod 2.$$

Karena m, n ganjil, maka terdapat m', n' dimana $m = 2m'+1, n = 2n'+1$, jadi

$$\begin{aligned}
\frac{m^2-1}{8} + \frac{n^2-1}{8} &= \frac{(2m'+1)^2-1}{8} + \frac{(2n'+1)^2-1}{8}\\
&= \frac{(4m'^2+4m'+1)-1}{8} + \frac{(4n'^2+4n'+1)-1}{8}\\
&= \frac{4m'^2+4m'}{8} + \frac{4n'^2+4n'}{8}\\
&= \frac{4m'^2+4m'+4n'^2+4n'}{8}.
\end{aligned}$$

Kita juga dapatkan

$$\begin{aligned}
\frac{m^2n^2-1}{8} &= \frac{(2m'+1)^2(2n'+1)^2-1}{8}\\
&= \frac{(4m'^2+4m'+1)(4n'^2+4n'+1)-1}{8}\\
&= 2(m'^2n'^2+m'^2n'+m'n'^2+m'n') + \frac{4m'^2+4m'+4n'^2+4n'}{8}\\
&\equiv \frac{4m'^2+4m'+4n'^2+4n'}{8} \pmod 2.
\end{aligned}$$

Jadi

$$\frac{m^2-1}{8} + \frac{n^2-1}{8} \equiv \frac{m^2n^2-1}{8} \pmod 2.$$

Karena produk bilangan ganjil juga ganjil, maka kita dapatkan

$$\frac{n_1^2-1}{8} + \ldots + \frac{n_m^2-1}{8} \equiv \frac{n_1^2\ldots n_m^2-1}{8} \pmod 2.$$

Kembali ke persamaan 11.15:

$$\begin{aligned}
\left(\frac{2}{n}\right) &= \left(\frac{2}{p_1}\right)^{\alpha_1}\ldots\left(\frac{2}{p_m}\right)^{\alpha_m}\\
&= ((-1)^{(p_1^2-1)/8})^{\alpha_1}\ldots((-1)^{(p_m^2-1)/8})^{\alpha_m}\\
&= ((-1)^{\alpha_1(p_1^2-1)/8})\ldots((-1)^{\alpha_m(p_m^2-1)/8})\\
&= (-1)^k
\end{aligned}$$

dengan $k = \sum_{i=1}^{k} \alpha_i (p_i^2 - 1)/8$, jadi

$$\begin{aligned}
k &= \underbrace{(p_1^2-1)/8 + \ldots + (p_1^2-1)/8}_{\alpha_1\times} + \ldots + \underbrace{(p_m^2-1)/8 + \ldots + (p_m^2-1)/8}_{\alpha_m\times} \\
&\equiv (\underbrace{p_1^2 \ldots p_1^2}_{\alpha_1\times} \ldots \underbrace{p_m^2 \ldots p_m^2}_{\alpha_m\times} - 1)/8 \pmod 2 \\
&\equiv ((p_1^{\alpha_1})^2 \ldots (p_m^{\alpha_m})^2 - 1)/8 \pmod 2 \\
&\equiv (n^2-1)/8 \pmod 2.
\end{aligned}$$

Jadi karena $(-1)^k = (-1)^{(n^2-1)/8}$, kita dapatkan

$$\left(\frac{-1}{n}\right) = (-1)^{(n^2-1)/8}.$$

Selesailah pembuktian persamaan 11.15. Untuk pembuktian persamaan 11.16, kita uraikan a dan n:

$$\begin{aligned}
a &= p_1 p_2 \ldots p_k \\
n &= q_1 q_2 \ldots q_l
\end{aligned}$$

dimana setiap p_i dengan $1 \le i \le k$ dan q_j dengan $1 \le j \le l$ merupakan bilangan prima, jadi pangkat bilangan prima telah diuraikan. Maka

$$\begin{aligned}
\left(\frac{a}{n}\right)\left(\frac{n}{a}\right) &= \prod_{i=1}^{k}\prod_{j=1}^{l}\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) \\
&= (-1)^{k_1 k_2}
\end{aligned}$$

dimana

$$\begin{aligned}
k_1 &= \sum_{i=1}^{k} \frac{p_i - 1}{2} \\
&\equiv (a-1)/2 \pmod 2, \text{ dan} \\
k_2 &= \sum_{j=1}^{l} \frac{q_j - 1}{2} \\
&\equiv (n-1)/2 \pmod 2.
\end{aligned}$$

Jadi

$$\left(\frac{a}{n}\right)\left(\frac{n}{a}\right) = (-1)^{\frac{a-1}{2}\frac{n-1}{2}}$$

dan selesailah pembuktian persamaan 11.16.

Persamaan 11.16 dapat digunakan untuk membuktikan generalisasi dari *quadratic reciprocity*:

Teorema 57 *Untuk dua bilangan positif ganjil m dan n:*

$$\left(\frac{m}{n}\right) = (-1)^{(m-1)(n-1)/4}\left(\frac{n}{m}\right).$$

Jika $\gcd(m,n) \neq 1$ maka kedua sisi dari persamaan menghasilkan 0. Jika $\gcd(m,n) = 1$ kita gunakan persamaan 11.16, dan karena $\left(\frac{m}{n}\right)$ dan $\left(\frac{n}{m}\right)$ mempunyai nilai ± 1 maka $\left(\frac{m}{n}\right) = (-1)^{(m-1)(n-1)/4}\left(\frac{n}{m}\right)$.

Kita dapat menggunakan *quadratic reciprocity* untuk menentukan dengan cepat apakah suatu bilangan bulat a merupakan kuadrat modulo suatu bilangan prima p. Sebagai contoh, kita periksa apakah 7411 merupakan suatu kuadrat modulo bilangan prima 9283. Karena $7411 \equiv 9283 \equiv 3 \pmod 4$ maka

$$\begin{aligned}
\left(\frac{7411}{9283}\right) &= -\left(\frac{9283}{7411}\right)\\
&= -\left(\frac{1872}{7411}\right)\\
&= -\left(\frac{16}{7411}\right)\left(\frac{117}{7411}\right)\\
&= -\left(\frac{117}{7411}\right)\\
&= -\left(\frac{7411}{117}\right)\\
&= -\left(\frac{40}{117}\right)\\
&= -\left(\frac{4}{117}\right)\left(\frac{2}{117}\right)\left(\frac{5}{117}\right)\\
&= -\left(\frac{2}{117}\right)\left(\frac{5}{117}\right)\\
&= \left(\frac{5}{117}\right)\\
&= \left(\frac{117}{5}\right)\\
&= \left(\frac{2}{5}\right)\\
&= -1.
\end{aligned}$$

Jadi 7411 bukan merupakan kuadrat modulo 9283.

11.2 Akar Kuadrat Modulo Bilangan Ganjil

Dengan menggunakan *quadratic reciprocity* kita dapat dengan cepat menentukan apakah suatu bilangan merupakan kuadrat modulo bilangan prima tertentu. Akan tetapi, untuk mencari akar dari kuadrat tersebut, kita tidak dapat menggunakan *quadratic reciprocity.* Kita akan bahas metode yang dapat digunakan untuk mencari akar tersebut. Jika p merupakan bilangan prima ganjil dan a merupakan suatu kuadrat modulo p, jadi

$$\left(\frac{a}{p}\right) = 1,$$

maka kita ingin dapatkan x dimana $x^2 \equiv a \pmod p$. Pertama, kita tulis $p-1$ dalam bentuk

$$p - 1 = 2^\alpha \cdot s,$$

dimana s adalah bilangan ganjil, jadi s didapat dengan membagi $p-1$ dengan 2 berulang kali hingga tidak dapat dibagi 2 lagi. Maka

$$r = a^{(s+1)/2} \pmod p$$

sudah mendekati akar dari a. Persisnya

$$\begin{aligned} (a^{-1}r^2)^{2^{\alpha-1}} &\equiv a^{s2^{\alpha-1}} \pmod p \\ &\equiv a^{(p-1)/2} \pmod p \\ &\equiv \left(\frac{a}{p}\right) \pmod p \\ &= 1. \end{aligned}$$

Jadi rasio r^2/a jika dipangkatkan $2^{\alpha-1}$ menghasilkan 1. Yang kita inginkan adalah rasio x^2/a sama dengan 1. Seberapa dekat nilai r dari x? Ini tergantung dari nilai p, jika $p \equiv 3 \pmod 4$ maka $\alpha = 1$, jadi nilai r dan x sama. Jika tidak, maka langkah-langkah berikut dapat digunakan untuk mendapatkan nilai x dari nilai r.

Secara garis besar, kita harus kalikan r dengan suatu akar pangkat 2^α dari 1 untuk mendapatkan x sehingga $(x^2/a) = 1$. Kita cari akar pangkat 2^α pengali ini menggunakan akar primitif pangkat 2^α sebagai patokan. Pertama, kita cari bilangan n yang merupakan *quadratic non-residue* modulo p, jadi

$$\left(\frac{n}{p}\right) = -1.$$

Jika kita buat

$$b \equiv n^s \pmod p$$

maka b merupakan akar pangkat 2^α dari 1 yang primitif (setiap akar pangkat 2^α dari 1, termasuk juga setiap akar pangkat 2^i dari 1 dimana $0 \leq i \leq \alpha$, dapat ditulis dalam bentuk pemangkatan b). Mari kita buktikan ini. Karena

$$\begin{aligned} b^{2^\alpha} &\equiv n^{2^\alpha s} \pmod p \\ &\equiv n^{p-1} \pmod p \\ &\equiv 1 \pmod p \end{aligned}$$

maka jelas b merupakan akar pangkat 2^α dari 1. Untuk menunjukkan bahwa b merupakan akar primitif, kita periksa apa konsekuensinya jika b bukan akar primitif: ada pemangkatan $b^i \equiv 1 \pmod p$ dimana $1 < i < 2^\alpha$, jadi $i|2^\alpha$ dan i genap, dan b sendiri adalah pemangkatan genap $(2^\alpha/i)$ dari akar primitif. Tetapi ini adalah kontradiksi karena jika b adalah hasil pemangkatan genap, maka b merupakan suatu kuadrat, sedangkan

$$\left(\frac{b}{p}\right) = \left(\frac{n}{p}\right)^s = -1$$

karena s adalah bilangan ganjil dan n adalah *non-residue*. Jadi b harus merupakan akar primitif.

Jadi kita gunakan b, yang merupakan akar primitif pangkat 2^α dari 1, sebagai patokan. Pengali r untuk mendapatkan x harus merupakan pemangkatan b, kita sebut saja b^j. Kita dapat umpamakan bahwa $j < 2^{\alpha-1}$ karena $b^{2^{\alpha-1}} = -1$, jadi j dapat ditambah dengan $2^{\alpha-1}$ untuk mendapatkan akar kuadrat yang satu lagi. Berikut cara mendapatkan j dengan satu persatu mencari bit $j_0, j_1, \ldots, j_{\alpha-2}$ secara induktif.

1. Kita pangkatkan (r^2/a) dengan $2^{\alpha-2}$ modulo p. Karena kita telah buktikan bahwa kuadrat bilangan ini adalah 1, maka bilangan ini adalah ± 1. Jika bilangan ini adalah 1 maka nilai j_0 adalah 0, sedangkan jika bilangan ini adalah -1 maka nilai j_o adalah 1.

2. Jika bit $j_0, j_1, \ldots, j_{k-1}$ telah didapat, maka $(b^{j_0+j_1+\ldots+j_{k-1}}r)^2/a$ merupakan akar pangkat $2^{\alpha-k-1}$ dari 1, jadi jika kita pangkatkan bilangan ini dengan $2^{\alpha-k-2}$ kita akan dapatkan ± 1. Jika kita dapatkan 1 maka nilai j_k adalah 0, sedangkan jika kita dapatkan -1 maka nilai j_k adalah 1.

Setiap kali kita selesai dengan langkah 2 untuk suatu k, maka

$$(b^{j_0+2j_1+\ldots+2^k j_k}r)^2/a$$

adalah akar pangkat $2^{\alpha-k-2}$ dari 1, jadi kita semakin dekat dengan solusi untuk akar kuadrat, dan saat kita selesai dengan $k = \alpha - 2$, maka

$$(b^{j_0+2j_1+\ldots+2^{\alpha-2}j_{\alpha-2}}r)^2/a = 1,$$

jadi $b^j r$ merupakan akar kuadrat dari a modulo p, dimana $j = j_0 + 2j_1 + \ldots + 2^{\alpha-2} j_{\alpha-2}$.

Mari kita coba gunakan metode diatas untuk mencari akar kuadrat dari 186 modulo 401, jadi $a = 186$, $p = 401$ dan $a^{-1} \equiv 235 \pmod{401}$. Kita temukan $n = 3$ merupakan *non-residue*, dan $p - 1 = 2^4 \cdot 25$, jadi $\alpha = 4$, $s = 25$,

$$b \equiv 3^{25} \equiv 268 \pmod{401}$$

dan

$$r \equiv 186^{13} \equiv 103 \pmod{401}.$$

Jadi $r^2/a \equiv 98 \pmod{401}$ yang merupakan akar pangkat $2^{\alpha-1} = 2^3 = 8$ dari 1. Kita lakukan langkah 1: $98^4 \equiv -1 \pmod{401}$, jadi $j_0 = 1$. Menggunakan langkah 2 kita dapatkan $j_1 = 0$ dan $j_2 = 1$, jadi $j = 1 + 2 \cdot 0 + 2^2 \cdot 1 = 5$. Jadi akar kuadrat dari 186 modulo 401 adalah

$$b^5 r \equiv 268^5 \cdot 103 \equiv 304 \pmod{401}.$$

Metode diatas adalah untuk mencari akar kuadrat modulo bilangan prima. Kita kembangkan metode diatas untuk mencari akar kuadrat modulo bilangan ganjil m yang telah diuraikan sebagai berikut:

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

dimana setiap p_i merupakan bilangan prima ganjil. Mari kita lihat bagaimana mencari solusi x untuk persamaan

$$x^2 \equiv a \pmod{m}.$$

Metode diatas dapat digunakan untuk mencari solusi x_0 untuk persamaan

$$x_0^2 \equiv a \pmod{p_i}$$

untuk setiap p_i. Selanjutnya, kita harus cari

$$x = x_0 + x_1 p_i + \cdots + x_{\alpha_i - 1} p_i^{\alpha_i - 1}$$

sehingga $x^2 \equiv a \pmod{p_i^{\alpha_i}}$. Kita gunakan induksi pada pangkat dari p_i. Untuk *base case* kita sudah dapatkan x_0. Untuk *step case*, jika kita sudah dapatkan bilangan berbasis p dengan $\alpha - 1$ *digit* $\hat{x}$ dimana $\hat{x}^2 \equiv a \pmod{p^{\alpha-1}}$, maka *digit* ke α dari

$$x = \hat{x} + x_{\alpha-1} p_i^{\alpha-1}$$

yaitu $x_{\alpha-1}$ dapat dicari, dimulai dengan menuliskan

$$\hat{x}^2 = a + b p_i^{\alpha-1}$$

untuk mendapatkan b. Jadi

$$\begin{aligned}
x^2 &= (\hat{x} + x_{\alpha-1}p_i^{\alpha-1})^2 \\
&= \hat{x}^2 + 2\hat{x}x_{\alpha-1}p_i^{\alpha-1} + x_{\alpha-1}^2 p_i^{2\alpha-2} \\
&\equiv \hat{x}^2 + 2\hat{x}x_{\alpha-1}p_i^{\alpha-1} \pmod{p_i^\alpha} \\
&\equiv a + p_i^{\alpha-1}(b + 2x_0x_{\alpha-1}) \pmod{p_i^\alpha}.
\end{aligned}$$

Jadi kita dapatkan $x_{\alpha-1} \equiv -(2x_0)^{-1}b \pmod{p}$. Untuk menggabungkan hasil dari setiap $p_i^{\alpha_i}$ kita dapat gunakan *Chinese Remainder Theorem*. Metode yang telah dikembangkan ini tentunya hanya dapat digunakan jika m telah diuraikan.

11.3 Ringkasan

Di bab ini kita telah bahas konsep *quadratic residue* dan metode untuk mencari akar kuadrat modulo bilangan ganjil. Konsep *quadratic residue* yaitu kuadrat modulo bilangan prima, digunakan dalam beberapa metode untuk test bilangan prima dan penguraian bilangan besar, sedangkan metode mencari akar kuadrat modulo bilangan ganjil digunakan dalam metode penguraian *quadratic sieve*.