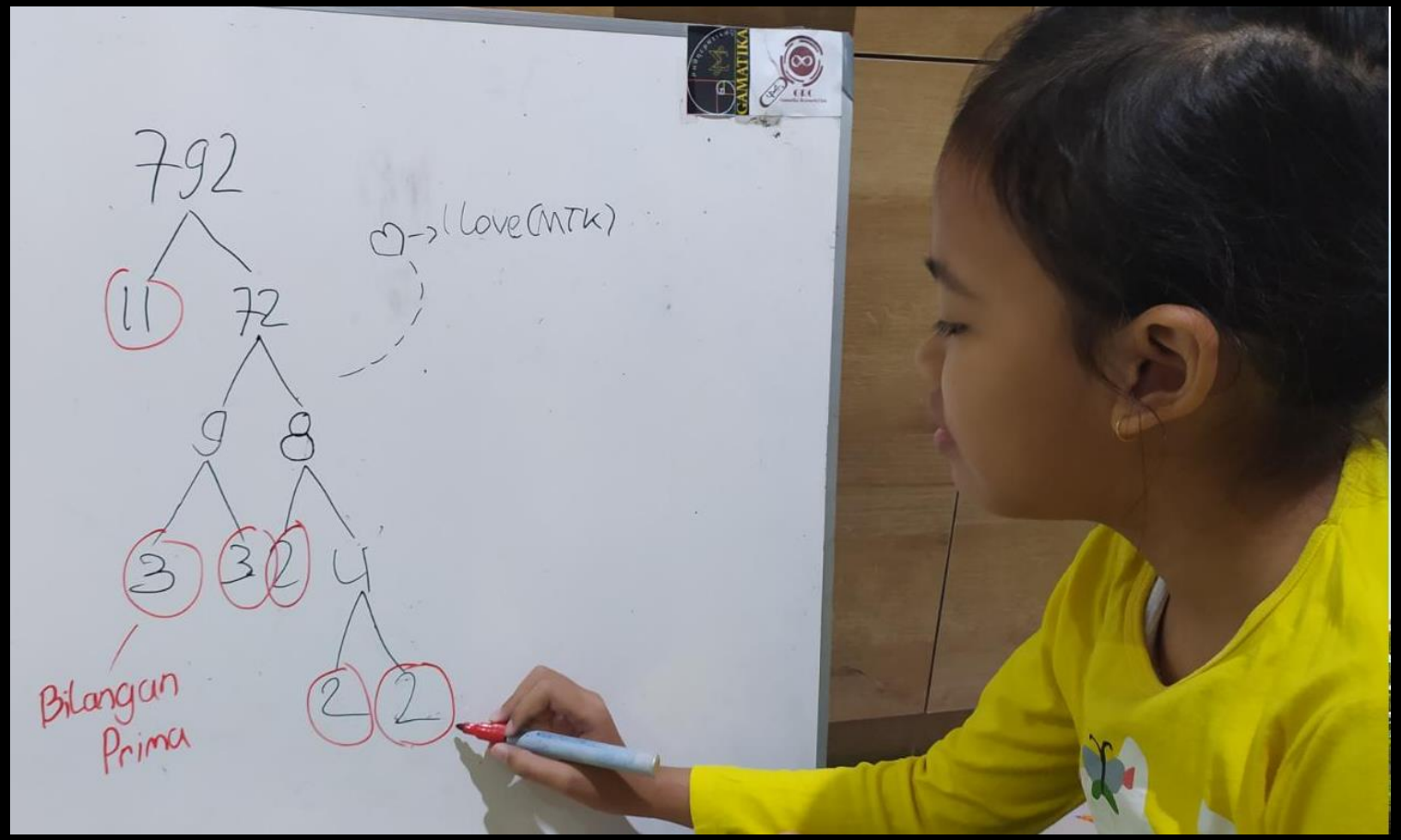
Ring Khusus

I Gede Adhitya Wisnu Wardhana

Universitas Mataram

Motivasi: The Power of $\mathbb{Z}$



Teorema Fundamental Aritmetika

Motivasi: The Power of $\mathbb{Z}$

- Apa itu bilangan prima?
- Di sekolah kita diajari bahwa bilangan prima adalah bilangan asli yang faktor positifnya hanya satu dan dirinya.
- Apa pentingnmya belajar bilangan prima?
- Sistem Keamanan digital saat ini memanfaatkan sifat-sifat bilangan prima
- Salah satu algoritma yang populer: RSA

Motivasi

- Apakah Faktor Prima dari 3139
- Butuh waktu cukup lama utk menemuk
- Bagaimana dengan 67349124013410311

Forbes

Quantum Computing Poses An Existential Security Threat, But Not Today

Wayne Rash Contributor

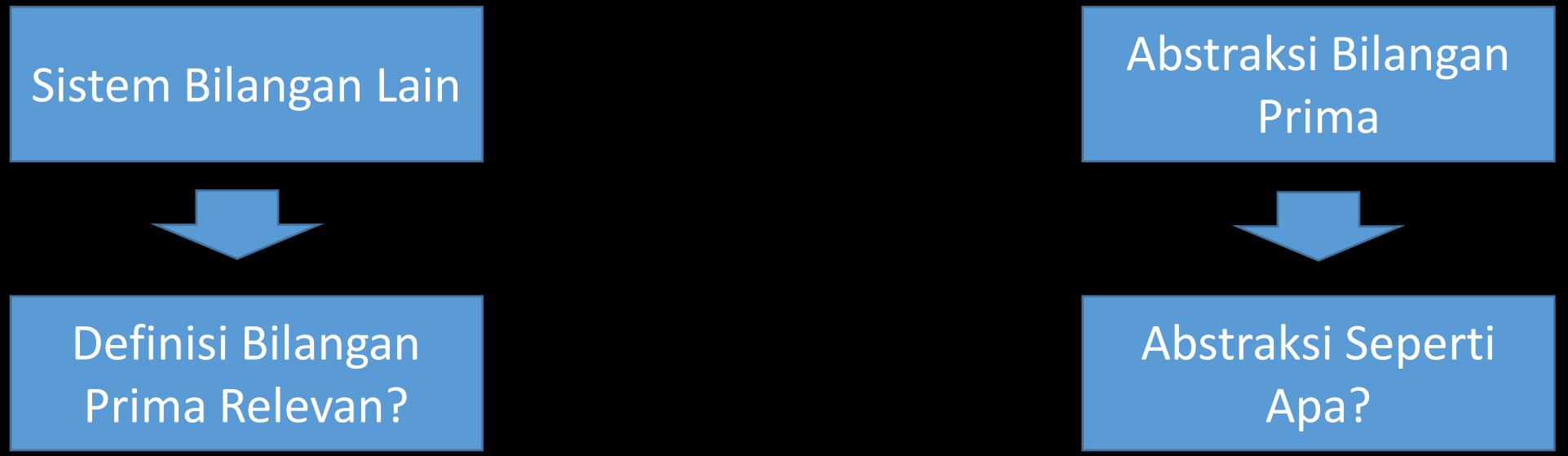
Consumer Tech

Wayne Rash is a technology and science writer based in Washington.

GETTY

Google's announcement on October 23, 2019 that its scientists has achieved quantum supremacy was

Motivasi: Menghadapi Komputer Kuantum



Pembagi Nol dan Bilangan Prima

- Jika m, $n \in \mathbb{Z}$ yang tak nol, kita tahu bahwa xy tak nol
- Tapi pada ring $\mathbb{Z}_6$, diketahui $\bar{2}.\bar{3} = \bar{0}$
- $\bar{2} \in \mathbb{Z}_6$ kita katakan pembagi nol $(\bar{2}|\bar{0})$

- Misalkan R ring komutatif, unsur tak nol $\mathrm{x} \in R$ dikatakan membagi y apabila $\exists c \in R$, sehingga $\mathrm{y} = xc$.
- Misalkan R ring komutatif, unsur tak nol $x \in R$ dikatakan ***pembagi nol*** apabila $\exists y \in R$ yang tak nol, sehingga $xy = 0$

Pembagi Nol dan Bilangan Prima

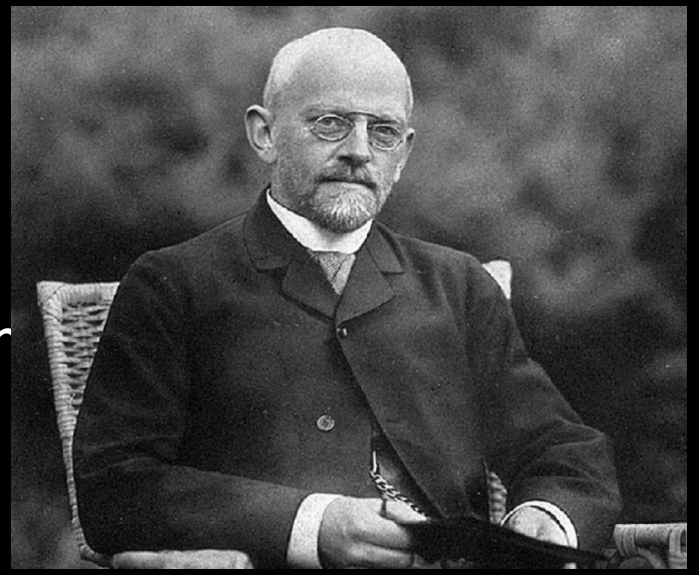
- Misalkan R ring komutatif dengan unsur kesatuan (1_R)
- $x \in R$ dikatakan ***unit*** apabila $\exists y \in R$ sehingga $xy = 1_R$
- $a, b \in R$ dikatakan berasosiasi apabila terdapat unit $u \in R$ sehingga $a = ub$
- $x \in R$ dikatkan tak tereduksi apabila untuk setiap $a, b \in R$ dimana $x = ab$, maka a unit atau b unit.

Pembagi Nol dan Bilangan Prima

- Misalkan R ring komutatif dengan unsur kesatuan (1_R)
- $p \in R$ bukan unit dikatakan prima, jika untuk setiap $a, b \in R$ dimana $p|ab$ berlaku $p|a$ atau $p|b$

- Misalkan $R = \mathbb{Z}$ dan p prima
- Apabila a adalah faktor p maka $p = ca$ untuk $c \in \mathbb{Z}$
- Menurut definisi $p|a$ atau $p|c$
- Apabila $p|a$ maka haruslah $p = a$ (dan $c = 1$)

Daerah Integral



- Misalkan R Ring komutatif dengan 1_R
- R dikatakan daerah integral apabila R tidak mem

- History: kenapa dikatakan daerah integral?
- Pada tahun 1897 David Hilbert menulis paper tentang struktur seperti bilangan bulat yang dianamakan ***Integritatsbereich*** pada jurnal ***Zahlbereich***.

Hukum Pembatalan Pada Daerah Integral

- Pada daerah integral D berlaku hukum pembatalan
- Artinya $\forall a, b, c \in D$, $a \neq 0$, dengan $ab = ac$, maka berlaku $b = c$
- Bukti:
- Misalkan $ab = ac$
- Maka $a(b - c) = 0$
- $a \neq 0$ dan D daerah integral
- Maka $b - c = 0$
- Jadi $b = c$

Bilangan Prima dan Bilangan Tak Tereduksi

- Pada Daerah Integral: Jika p bilangan prima, maka p tak tereduksi
- Bukti:
- Asumsikan p bilangan prima
- Misalkan $a, b \in R$ sebarang sehingga $p = ab$
- Karena p prima maka $p|a$ atau $p|b$
- Jika $p|a$ maka $a = pc$
- Akibatnya $p = pcb$
- Berdasarkan hukum pembatalan $cb = 1$
- b unit

Bilangan Prima dan Bilangan Tak Tereduksi

- Bilangan tak tereduksi belum tentu prima?
- Misal $R = \langle x^2, y^2, xy \rangle$
- xy tak tereduksi di R
- $xy | x^2y^2$ tapi tidak membagi salah satunya
- Jadi xy bukan bilangan prima

Bilangan Bulat Gauss

- Bilangan bulat Gaus, $\mathbb{Z}[i] = \{a + ib | a, b \in \mathbb{Z}, i^2 = -1\}$
- Jelas $\mathbb{Z} \subset \mathbb{Z}[i]$
- Menariknya 2 bukan bilangan prima di $\mathbb{Z}[i]$
- $2 = (1 + i)(1 - i)$
- Bagaimana bentuk bilangan prima pada $\mathbb{Z}[i]$?

[Fariz Maulana, *Ekivalensi Ideal Hampir Prima dan Ideal Prima Pada Bilangan Bulat Gauss, Eigen Mathemathics Journal, Vol 2 [1], 2019]*

Lapangan

- Misalkan R Ring komutatif dengan 1_R
- R dikatakan lapangan apabila setiap unsur tak nolnya adalah unit.

- Misalkan a unit di R
- Apabila $ab = 0$
- Maka $a^{-1}(ab) = 0$
- $b = 0$
- Jadi a bukan pembagi nol
- Lapangan adalah Daerah Integral

Lapangan

- $\mathbb{Z}$ Adalah daerah integral yang bukan lapanagan
- Artinya lapangan dan daerah integral adalah dua struktur yang berbeda
- Tapi jika Ring berhingga, maka keduanya ekivalen
- Misalkan $\mathrm{R} = \{a_1, a_2, \dots, a_n\}$ adalah daerah integral
- Untuk sebarang $a \in R$ tak nol, kita buat himpunan $\{aa_1, aa_2, \dots aa_n\}$
- $aa_i \neq aa_j$ karena hukum pembatalan
- $aa_k = 1$
- Jadi R lapangan.

Ideal Prima dan Ideal Maksimal


1921


1877

- Ideal sejati I dari ring R dikatakan ideal prima apabila untuk setiap ideal A, B dari R dengan $AB \subset I$ berakibat $A \subset I$ atau $B \subset I$.
- Untuk R ring komutatif, Ideal sejati I dikatakan ideal prima apabila $\forall a, b \in R$ dengan $ab \in I$ berakibat $a \in I$ atau b $\in I$.

- Perhatikan bahwa definisi yang kedua itu lebih kuat sehingga sering dikatakan ideal prima kuat.
- Perhatikan ring matriks, ideal nol merupaka ideal prima tapi bukan ideal prima kuat.

Ideal Prima dan Ideal Maksimal

- Misalkan R ring komutatif dengan 1_R
- Ideal sejati P di R adalah ideal prima $\Leftrightarrow$ R/P daerah integral
- $\Leftarrow$ Misalkan $a, b \in R$ dengan $ab \in P$
- Akibatnya $(a + P)(b + P) = ab + P = 0 + P$
- Karena R/P daerah integral, maka $(a + P) = 0$ atau $(b + P) = 0$
- Artinya $a \in P$ atau $b \in P$
- Jadi P ideal prima

Ideal Prima dan Ideal Maksimal

- Misalkan R ring komutatif dengan 1_R
- Ideal sejati P di R adalah ideal prima $\Leftrightarrow R/P$ daerah integral
- $\Rightarrow$ Misalkan $(a+P)(b+P) = 0 + \mathrm{P}$
- $ab + P = 0 + P$
- $ab \in P$
- $a \in P$ atau $b \in P$
- $a + P = 0 + P$ atau $b + P = 0 + P$
- R daerah integral

Ideal Prima dan Ideal Maksimal

- Misalkan R ring dan M ideal sejati
- M ideal maksimal jika tidak ada ideal I sehingga $M \subset I \subset R$

- M ideal maksimal jika untuk semua ideal I dengan $M \subseteq I \subseteq R$ berlaku $I = M$ atau $I = R$

Ideal Prima dan Ideal Maksimal

- Misalkan R ring komutatif dengan 1_R
- Ideal sejati M di R adalah ideal maksimal $\Leftrightarrow$ R/M lapangan
- $\Rightarrow$ Misal M ideal maksimal
- $a + M \in R/M$ tak nol akibatnya $a \notin M$
- Sehingga $\langle M \cup \{a\} \rangle = R$
- $1_R = m + ra$
- $1 + M = ra + M = (r + M)(a + M)$
- R/M lapangan

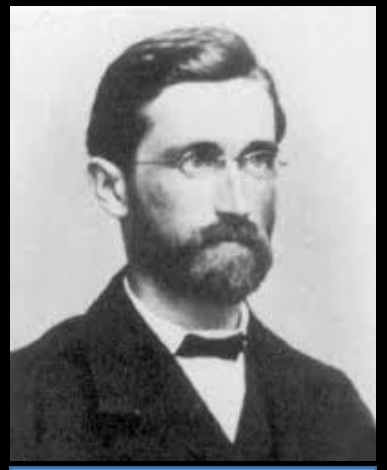
Ideal Prima dan Ideal Maksimal

- Misalkan R ring komutatif dengan 1_R
- Ideal sejati M di R adalah ideal maksimal $\Leftrightarrow R/M$ lapangan
- $\Leftarrow$ Misal R/M lapangan
- Misal ideal I memenuhi $M \subset I \subseteq R$
- $\exists x \in I$ dengan $x \notin M$
- $x + M$ tak nol, jadi suatu unit
- $(x + M)(y + M) = xy + M = 1 + M$
- $1_R - xy \in M \rightarrow 1_R = xy + m \in I$

Ideal Prima dan Ideal Maksimal

- Pada ring $\mathbb{Z}$, Ideal $\{0\}$ adalah ideal prima, tapi bukan ideal maksimal
- Bagaimana sebaliknya?
- Misalkan R ring komutatif dengan 1_R dan M ideal maksimal dari R
- Misalkan $ab \in M$, asumsikan $a \notin M$
- Ideal $\{m + ra | m \in M, r \in R\}$ memuat ideal M tapi tidak sama
- Karena M maksimal $\{m + ra | m \in M, r \in R\} = R$
- $1_R = m' + r'a \Rightarrow b = bm' + r'ab = bm' + m" \in M$
- M ideal prima

Riset Terkait Keprimaan Ideal



Ideal Prima
1877

Ideal Hampir Prima
2009

Submodulr Prima
1978

Submodul Hampir Prima
2012

Semoga Bermanfaat