Order dari sebuah Elemen

Wildan Bagus Wicaksono

Diperbarui 18 Mei 2022

Topik yang dibahas kali ini mengenai *Order dari sebuah Elemen* yang terkait dengan modular aritmetika. Sebelum membaca, setidaknya Anda telah menguasai keterbagian, dasar modular aritmetika, Teorema Euler, dan Teorema Fermat.

Daftar Isi

1 Definisi dan Teorema Order 1

2 Akar Primitif (Primitive Root) 2

3 Contoh Soal 7

4 Latihan Soal 10

5 Petunjuk 13

6 Solusi Soal Terpilih 15

§1 Definisi dan Teorema Order

Misalkan a bilangan bulat dan b bilangan asli. Maka **order** dari a modulo b adalah bilangan asli terkecil k yang memenuhi

$$a^k \equiv 1 \pmod{b}.$$

Biasanya dituliskan sebagai $\text{ord}_b(a) = k$ atau $o_b(a) = k$. Sebagai contoh, $\text{ord}_7(5) = 6$ karena

$$5^1 \equiv 5 \pmod 7, \quad 5^2 \equiv 4 \pmod 7, \quad 5^3 \equiv 6 \pmod 7,$$
$$5^4 \equiv 2 \pmod 7, \quad 5^5 \equiv 3 \pmod 7, \quad 5^6 \equiv 1 \pmod 7.$$

Di sini saya akan memakai $\text{ord}_b(a) = k$ sebagai penulisan order dari $a \pmod b$.

Teorema 1.1 (Order dari sebuah Elemen)

Diberikan a dan b bilangan bulat serta $b > 0$. Maka $a^m \equiv 1 \pmod b$ jika dan hanya jika $\text{ord}_b(a) \mid m$.

Bukti. Pembuktian dari kiri ke kanan. Andaikan ada m di mana $\text{ord}_b(a) \nmid m$. Misalkan $\text{ord}_b(a) = x$. Misalkan pula $m = nx + \theta$ di mana $n \in \mathbb{Z}$ dan $0 < \theta < x$. Kita punya

$$1 \equiv a^m \equiv a^{nx+\theta} \equiv (a^x)^n \cdot a^\theta \equiv 1^n \cdot a^\theta \equiv a^\theta \pmod b.$$

Hal ini kontradiksi karena terdapat bilangan $\theta < \text{ord}_b(a)$ yang memenuhi $a^\theta \equiv 1 \pmod b$. Maka haruslah $\theta = 0 \iff \text{ord}_b(a) \mid m$.
Pembuktian dari kanan ke kiri. Misalkan $\text{ord}_b(a) = x$ dan misalkan $m = nx$ di mana $n \in \mathbb{Z}$. Maka

$$a^m \equiv a^{nx} \equiv (a^x)^n \equiv 1^n \equiv 1 \pmod b.$$

Jadi, terbukti bahwa $a^m \equiv 1 \pmod b$ jika dan hanya jika $\text{ord}_b(a) \mid m$. □

Exercise 1.2. Buktikan bahwa $a \pmod b$ memiliki order jika dan hanya jika $\gcd(a, b) = 1$.

Lemma 1.3

Misalkan a bilangan bulat dan b bilangan asli di mana $\gcd(a, b) = 1$. Maka $\text{ord}_b(a) \mid \varphi(b)$. Secara khusus, untuk b bilangan prima berlaku $\text{ord}_b(a) \mid b - 1$.

Bukti. Dari **Teorema Euler (Teorema 1.4)**, berlaku $a^{\varphi(b)} \equiv 1 \pmod b$. Dari **Teorema 1.1**, berlaku $\text{ord}_b(a) \mid \varphi(b)$. Secara khusus, jika b bilangan prima berlaku $\varphi(b) = b - 1$ dan kita peroleh yang diminta. □

Teorema 1.4 (Euler)

Jika a dan p dua bilangan bulat yang relatif prima di mana $p > 0$, maka $a^{\varphi(p)} \equiv 1 \pmod p$.

§2 Akar Primitif (Primitive Root)

Misalkan n bilangan asli. Suatu bilangan bulat g dengan $\gcd(g, n) = 1$, disebut **akar primitif**, sehingga order dari $g \pmod n$ adalah $\varphi(n)$.

Teorema 2.1 (Eksistensi Akar Primitif)

Suatu bilangan asli n memiliki akar primtif modulo n jika dan hanya jika $n = 2$, $n = 4$, $n = p^k$, atau $n = 2p^k$ untuk suatu bilangan prima ganjil p dan bilangan asli k.

Bukti. Kita bagi dua kasus: $n = 2^k$ dan $n = mp^k$ untuk suatu bilangan asli m dengan $\gcd(m, p) = 1$.
Kasus 1. Jika $n = 2^k$ untuk suatu bilangan asli k. Jika $n = 2$, ambil $g = 3$, jelas $3^1 \equiv 1 \pmod 2 \implies g^{\varphi(2)} \equiv 1 \pmod 2$. Jika $n = 4$, ambil $g = 3$ memenuhi karena

$$3^1 \equiv 3 \pmod 4, \quad 3^2 \equiv 1 \pmod 4 \implies 3^{\varphi(4)} \equiv 1 \pmod 4.$$

Akan kita buktikan untuk setiap $k \geq 3$, maka n tidak memiliki akar primitif modulo n. Akan kita buktikan dengan induksi. Untuk setiap bilangan ganjil a berlaku $a^2 \equiv 1 \pmod 8$. Artinya, untuk $n = 8$ tidak memiliki akar primitif modulo n. Tinjau $\varphi\left(2^k\right) = 2^k\left(1 - \frac{1}{2}\right) = 2^{k-1}$. Kita klaim bahwa terdapat $\alpha < 2^{k-1}$ sehingga $2^\alpha \equiv 1 \pmod{2^k}$. Sekarang, akan kita tunjukkan bahwa

$$a^{2^{k-2}} \equiv 1 \pmod{2^k}$$

untuk setiap bilangan ganjil a dengan menggunakan induksi. Jika $k = 3$, maka $a^2 \equiv 1 \pmod 8$ yang mana benar. Asumsikan untuk suatu $k = l$, maka $a^{2^{l-2}} \equiv 1 \pmod{2^l}$. Misalkan $a^{2^{l-2}} = 2^l b + 1$ untuk suatu bilangan bulat tak negatif b. Untuk $k = l + 1$,

$$a^{2^{l-1}} = \left(a^{2^{l-2}}\right)^2 = \left(2^l b + 1\right)^2 = 2^{2l}b^2 + 2^{l+1}b + 1 \equiv 1 \pmod{2^{l+1}} \implies a^{2^{l-1}} \equiv 1 \pmod{2^{l+1}}.$$

Maka untuk $k = l + 1$ juga benar dan menurut induksi terbukti bahwa untuk setiap $k \geq 3$, berlaku $a^{2^{k-2}} \equiv 1 \pmod{2^k}$ untuk setiap bilangan ganjil a. Jadi, $n = 2^k$ untuk setiap $k \geq 3$ tidak memiliki akar primitif modulo n.

> **Remark.** Selain menggunakan induksi dapat menggunakan Lifting The Exponent, yaitu
>
> $$\nu_2\left(a^{2^{k-2}} - 1\right) = \nu_2\left(a^2 - 1\right) + \nu_2\left(2^{k-2}\right) - 1 \geq 3 + k - 2 - 1 = k$$
>
> dan diperoleh $2^k \mid a^{2^{k-2}} - 1$.

Kasus 2. Jika $n = mp^k$ untuk suatu bilangan asli k dan m di mana $\gcd(m, p) = 1$ serta p prima ganjil. Akan kita tunjukkan untuk $m = 1$ dan $m = 2$, maka n memiliki akar primitif modulo n. Kita mulai dengan lemma berikut.

Lemma 2.2

Jika r akar primitif modulo p di mana p bilangan prima ganjil, maka salah satu dari r atau $r + p$ merupakan akar primitif modulo p^2.

Perhatikan bahwa $r = \varphi(p) \implies r = p - 1$. Misalkan $\text{ord}_{p^2}(r) = x$, maka $r^x \equiv 1 \pmod{p^2}$. Kita punya juga $r^x \equiv 1 \pmod{p}$. Dari **Teorema 1.1**, maka $\text{ord}_p(r) \mid x \implies p - 1 \mid x$. Sedangkan, dari **Lemma 1.3**, maka $\text{ord}_{p^2}(r) \mid \varphi\left(p^2\right) \implies x \mid p(p-1)$. Mengingat $p - 1 \mid x$, maka haruslah $x = p - 1$ atau $x = p(p-1)$.

- Jika $x = p(p-1) = \varphi\left(p^2\right) \implies \text{ord}_{p^2}(r) = \varphi\left(p^2\right)$, maka r adalah akar primitif modulo p^2.
- Jika $x = p - 1$, maka $r^{p-1} \equiv 1 \pmod{p^2}$. Misalkan $s = r + p$, maka s juga merupakan akar primitif modulo p (mengapa?). Dengan cara yang sama, diperoleh $\text{ord}_{p^2}(s) = p - 1$ atau $\text{ord}_{p^2}(s) = p(p-1)$. Akan kita tunjukkan $\text{ord}_{p^2}(s) \neq p - 1$. Andaikan $\text{ord}_{p^2}(s) = p - 1$. Perhatikan bahwa

$$\begin{aligned} s^{p-1} = (r+p)^{p-1} &= \sum_{i=0}^{p-1} \binom{p-1}{i} r^{p-1-i} p^i \\ &\equiv r^{p-1} + (p-1)pr^{p-2} \pmod{p^2} \\ &\equiv r^{p-1} + \left(p^2 - p\right) r^{p-2} \pmod{p^2} \\ &\equiv 1 - pr^{p-2} \pmod{p^2}. \end{aligned}$$

  Maka $p^2 \mid s^{p-1} - 1 + pr^{p-2}$. Karena $s^{p-1} - 1 \equiv 0 \pmod{p^2}$, maka $p^2 \mid pr^{p-2} \iff p \mid r^{p-2}$. Padahal $p \nmid r$, kontradiksi bahwa $p \mid r^{p-2}$. Kita punya $\text{ord}_{p^2}(s) = p(p-1) = \varphi\left(p^2\right)$ sehingga s merupakan akar primitif modulo p^2.

Lemma terbukti. Sekarang, akan kita buktikan bahwa $n = p^k$ atau $n = 2p^k$ memiliki akar primitif modulo n, sedangkan $n = mp^k$ untuk $m \geq 3$ dan $\gcd(m, p) = 1$ tidak memiliki akar primitif modulo n.

Subkasus 2.1. Akan kita buktikan bahwa $n = p^k$ memiliki akar primitif modulo n.

Lemma 2.3

Jika r akar primitif modulo p, maka r akar primitif modulo p^m untuk setiap bilangan asli m.

Dari **Lemma 2.2**, jika r akar primitif modulo p maka r juga akar primitif modulo p^2. Kita punya $r^{p-1} \not\equiv 1 \pmod{p^2}$ dan $r^{p(p-1)} \equiv 1 \pmod{p^2}$. Sekarang, akan kita buktikan dengan induksi bahwa untuk setiap bilangan asli $m \geq 2$, kita punya

$$r^{\varphi(p^m)} = r^{p^{m-1}(p-1)} \equiv 1 \pmod{p^m} \quad \text{dan} \quad r^{p^{m-2}(p-1)} \not\equiv 1 \pmod{p^m}.$$

Untuk $m = 2$, diperoleh $r^{p(p-1)} \equiv 1 \pmod{p^2}$ dan $r^{p-1} \not\equiv 1 \pmod{p^2}$ yang mana benar. Asumsikan untuk suatu $m = k$ benar, maka

$$r^{p^{k-1}(p-1)} \equiv 1 \pmod{p^k} \quad \text{dan} \quad r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}.$$

Misalkan $r^{p^{k-1}(p-1)} = 1 + yp^k$ untuk suatu bilangan bulat tak negatif y dan $\gcd(y, p) = 1$. Maka

$$r^{p^k(p-1)} = \left(r^{p^{k-1}(p-1)}\right)^p = \left(1 + yp^k\right)^p = \sum_{i=0}^{p} \binom{p}{i} y^i p^{ki}.$$

Tinjau $k + 1 < ki \iff p^{k+1} \mid p^{ki}$ untuk setiap $i \geq 2$. Maka

$$r^{p^k(p-1)} = \sum_{i=0}^{p} \binom{p}{i} y^i p^{ki} \equiv 1 + \binom{p}{1} yp^k \equiv 1 + yp^{k+1} \equiv 1 \pmod{p^{k+1}}.$$

Maka $r^{p^k(p-1)} \equiv 1 \pmod{p^{k+1}}$, sedangkan kita punya juga

$$r^{p^{k-1}(p-1)} = 1 + yp^k \not\equiv 1 \pmod{p^{k+1}}$$

yang mana untuk $m = k + 1$ juga benar. Menurut induksi terbukti bahwa

$$r^{p^{m-1}(p-1)} \equiv 1 \pmod{p^m} \quad \text{dan} \quad r^{p^{m-2}(p-1)} \not\equiv 1 \pmod{p^m}.$$

Sekarang, akan kita buktikan bahwa r adalah akar primitif modulo p^m. Misalkan $t = \text{ord}_{p^m}(r)$. Dari **Teorema 1.1**, maka $t \mid p^{m-1}(p-1)$ dan $t \nmid p^{m-2}(p-1)$ sehingga haruslah $t = p^{m-1}q$. Tinjau $r^t \equiv 1 \pmod{p^m} \implies r^t \equiv 1 \pmod{p}$. Maka $\text{ord}_p(r) \mid t \implies p - 1 \mid t$ yang berarti $p - 1 \mid p^{m-1}q$. Karena $\gcd(p - 1, p) = 1$, kita punya $p - 1 \mid q$ yang artinya haruslah $q = p - 1$. Maka $\text{ord}_{p^m}(r) = p^{m-1}(p-1) = \varphi(p^m)$ sehingga r adalah akar primitif modulo p^m.

Subkasus 2.2. Akan kita buktikan $n = 2p^k$ memiliki akar primitif modulo n. Kita mulai dengan lemma berikut.

Lemma 2.4

Jika r adalah akar primitif ganjil modulo p^k, maka r juga akar primitif dari $2p^k$. Sedangkan, jika r adalah akar primitif genap modulo p^k, maka $r + p^s$ adalah akar primitif dari $2p^k$.

Tinjau $\text{ord}_{p^k}(r) = \varphi\left(p^k\right)$. Karena φ bersifat multiplikatif*, kita punya $\varphi\left(2p^k\right) = \varphi(2)\varphi\left(p^k\right) = \varphi\left(p^k\right)$. Maka $\text{ord}_{p^k}(r) = \varphi\left(2p^k\right)$ sehingga diperoleh $p^k \mid r^{\varphi\left(2p^k\right)} - 1$.

- Jika r ganjil, maka $2 \mid r^{\varphi\left(2p^k\right)} - 1$. Kita peroleh

  $$\text{KPK}\left(2, p^k\right) \mid r^{\varphi\left(2p^k\right)} - 1 \implies 2p^k \mid r^{\varphi\left(2p^k\right)} - 1.$$

  Apabila ada suatu bilangan $l < \varphi\left(2p^k\right)$, maka $l\varphi\left(p^k\right)$ sehingga $2p^k \mid r^l - 1 \implies p^k \mid r^l - 1$, hal ini kontradiksi bahwa r akar primitif modulo p^k. Kita simpulkan bahwa r juga akar primitif modulo $2p^k$.

- Jika r genap, maka $r + p^k$ ganjil. Misalkan $r + p^k = t$. Maka $2 \mid t^{\varphi\left(2p^k\right)} - 1$. Di sisi lain,

  $$t^{\varphi\left(2p^k\right)} = \left(r + p^k\right)^{\varphi\left(2p^k\right)} \equiv r^{\varphi\left(2p^k\right)} \equiv 1 \pmod{p^l} \implies p^k \mid t^{\varphi\left(2p^k\right)} - 1.$$

  Kita peroleh bahwa $2p^k \mid t^{\varphi\left(2p^k\right)} - 1$ dan dengan cara yang sama seperti sebelumnya, $t = r + p^k$ adalah akar primitif modulo $2p^k$.

*Jika a, b dua bilangan asli yang saling relatif prima, maka $\varphi(ab) = \varphi(a)\varphi(b)$. Dapat dibuktikan sebagai latihan.

Lemma terbukti. Dari **subkasus 2.1**, kita telah membuktikan p^k memiliki akar primitif untuk setiap bilangan asli k. Dari **Lemma 2.4**, maka $2p^k$ juga memiliki akar primitif untuk setiap bilangan asli k.

Subkasus 2.3. Jika n tidak berbentuk p^k atau $2p^k$. Misalkan $n = p_1^{k_1}p_2^{k_2}\cdots p_t^{k_t}$ di mana $p_1, p_2, \cdots, p_t$ bilangan prima yang berbeda dan $k_1, k_2, \cdots, k_t$ bilangan asli. Andaikan n memiliki akar primitif r, maka $\gcd(n, r) = 1$ dan $\text{ord}_n(r) = \varphi(n)$. Selain itu, kita punya $\gcd\left(r, p_i^{k_i}\right) = 1$ untuk setiap $1 \le i \le t$. Dari **Teorema 1.4**,

$$p_i^{k_i} \mid r^{\varphi\left(p_i^{k_i}\right)} - 1$$

untuk setiap $1 \le i \le t$. Misalkan $L = \text{KPK}\left(\varphi\left(p_1^{k_1}\right), \varphi\left(p_2^{k_2}\right), \cdots, \varphi\left(p_i^{k_i}\right)\right)$. Maka $p_i^{k_i} \mid r^L - 1$ untuk setiap $1 \le i \le k$. Kita punya

$$\text{KPK}\left(p_1^{k_1}, p_2^{k_2}, \cdots, p_t^{k_t}\right) \mid r^L - 1 \implies p_1^{k_1}p_2^{k_2}\cdots p_t^{k_t} \mid r^L - 1 \implies n \mid r^L - 1.$$

Kita peroleh $r^L \equiv 1 \pmod n$. Dari **Teorema 1.1**, maka $\text{ord}_n(r) \mid L \implies \text{ord}_n(r) \le L$ dan diperoleh $\varphi(n) \le L$. Kita punya

$$L \ge \varphi(n) = \varphi\left(p_1^{k_1}p_2^{k_2}\cdots p_t^{k_t}\right) = \varphi\left(p_1^{k_1}\right)\varphi\left(p_2^{k_2}\right)\cdots\varphi\left(p_t^{k_t}\right).$$

Padahal $L \le \varphi\left(p_1^{k_1}p_2^{k_2}\cdots p_t^{k_t}\right) = \varphi\left(p_1^{k_1}\right)\varphi\left(p_2^{k_2}\right)\cdots\varphi\left(p_t^{k_t}\right)$ sehingga harus $L = \varphi\left(p_1^{k_1}p_2^{k_2}\cdots p_t^{k_t}\right) = \varphi\left(p_1^{k_1}\right)\varphi\left(p_2^{k_2}\right)\cdots\varphi\left(p$
Kesamaan terjadi jika dan hanya jika $\gcd\left(\varphi\left(p_1^{k_1}\right), \varphi\left(p_2^{k_2}\right), \cdots, \varphi\left(p_t^{k_t}\right)\right) = 1$. Hal ini kontradiksi karena $\varphi(n)$ selalu bernilai genap untuk $n \ge 3$ (pembuktian diserahkan kepada pembaca sebagai latihan). Maka dalam hal ini n tidak memiliki akar primitif.

Jadi, n memiliki akar primitif jika dan hanya jika $n = 2, n = 4, n = p^k$, atau $n = 2p^k$ untuk suatu prima ganjil p dan bilangan asli k. □

Teorema 2.5 (Akar Primitif)

Misalkan r adalah akar primitif modulo n dan n bilangan asli serta $\gcd(r, n) = 1$. Misalkan pula $a_1, a_2, \cdots, a_{\varphi(n)}$ adalah semua bilangan asli yang tidak lebih dari n dan relatif prima dengan n. Maka

$$\left\{r^1, r^2, \cdots, r^{\varphi(n)}\right\} \pmod n = \left\{a_1, a_2, \cdots, a_{\varphi(n)}\right\}.$$

Dengan kata lain, untuk setiap $1 \le i \le \varphi(n)$ terdapat j sehingga $r^j \equiv a_i \pmod n$. Secara khusus, jika $n = p$ bilangan prima, maka

$$\left\{r^1, r^2, \cdots, r^{p-1}\right\} \pmod p = \{1, 2, \cdots, p-1\}.$$

Berikut penerapan dari penggunaan akar primitif.

Lemma 2.6

Diberikan p bilangan prima dan m bilangan bulat. Maka

$$1^m + 2^m + 3^m + \cdots + (p-1)^m \equiv \begin{cases} 0 \pmod p, & \text{jika } p-1 \nmid m \\ -1 \pmod p, & \text{jika } p-1 \mid m \end{cases}.$$

Bukti. Jika $p - 1 \mid m$, maka

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

Kita punya

$$\sum_{i=1}^{p-1} i^m \equiv \sum_{i=1}^{p-1} 1 \equiv p - 1 \equiv -1 \pmod p.$$

Jika $p-1 \nmid m$. Dari **Theorem 2.1**, maka p memiliki akar primitif modulo p, misalkan g. Maka

$$\sum_{i=1}^{p-1} i^m \equiv \sum_{i=1}^{p-1} g^{im} \equiv \frac{g^m\left(g^{p-1}-1\right)}{g^m-1} \equiv 0 \pmod{p}$$

karena $g^m - 1 \not\equiv 0 \pmod{p}$ dan $g^{p-1} - 1 \equiv 0 \pmod{p}$. □

Teorema 2.7 (Wolstenholme's)

Untuk bilangan prima $p > 3$, maka

$$(p-1)!\left(\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1}\right) \equiv 0 \pmod{p^2}.$$

Bukti. Karena $p \nmid (p-1)!$ dari **Teorema Wilson (Teorema 2.8)**, maka $\gcd\left(p^2,(p-1)!\right) = 1$. Kita tinggal menunjukkan

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1} \equiv 0 \pmod{p^2}$$

di mana $\frac{1}{1}, \frac{1}{2}, \cdots, \frac{1}{p-1} \pmod{p^2}$ menyatakan invers dari $1, 2, \cdots, p-1 \pmod{p^2}$. Kita punya

$$\sum_{i=1}^{p-1} \frac{1}{i} \equiv \frac{1}{2}\sum_{i=1}^{p-1}\left(\frac{1}{i}+\frac{1}{p-i}\right) \equiv \frac{1}{2}\sum_{i=1}^{p-1}\frac{p}{i(p-i)} \pmod{p^2}.$$

Kita tinggal membuktikan $\sum_{i=1}^{p-1} \frac{1}{i(p-i)} \equiv 0 \pmod{p}$. Dari **Lemma 2.6**, maka $\sum_{i=1}^{p-1} i^{-2} \equiv 0 \pmod{p}$. Sehingga

$$\sum_{i=1}^{p-1}\frac{1}{i(p-i)} \equiv \sum_{i=1}^{p-1}\frac{1}{i(-i)} \equiv -\sum_{i=1}^{p-1}\frac{1}{i^2} \equiv 0 \pmod{p}$$

dan kita peroleh seperti yang ingin dibuktikan. □

Teorema 2.8 (Wilson)

Jika p bilangan prima, maka $(p-1)! \equiv -1 \pmod{p}$.

§3 Contoh Soal

Contoh 3.1

Misalkan p_n adalah faktor prima terkecil dari n^8+1 untuk setiap bilangan asli n. Tentukan sisa pembagian $p_1 + p_2 + \cdots + p_{2022}$ jika dibagi 16.

Jika n ganjil, maka $p_n = 2$. Tinjau ketika n genap. Kita punya

$$n^8 \equiv -1 \pmod{p_n} \implies n^{16} \equiv 1 \pmod{p_n}.$$

Dari **Teorema 1.1**, maka $\text{ord}_{p_n}(n) \mid 16$. Maka $\text{ord}_{p_n}(n) \in \{1,2,4,8,16\}$. Karena $n^8 \not\equiv 1 \pmod{8}$, menurut **Teorema 1.1**, kita simpulkan bahwa $\text{ord}_{p_n}(n) \nmid 8$. Sehingga kita punya $\text{ord}_{p_n}(n) = 16$. Dari **Lemma 1.3**, maka $\text{ord}_{p_n}(n) \mid \varphi(p_n) \implies 16 \mid p_n - 1$. Maka $p_n \equiv 1 \pmod{16}$ untuk setiap n genap. Maka

$$p_1 + p_2 + \cdots + p_{2022} \equiv 1 \cdot 1011 + 2 \cdot 1011 \equiv 3 \cdot 1011 \equiv 3 \cdot 3 \equiv 9 \pmod{16}.$$

Jadi, sisa pembagian $p_1 + p_2 + \cdots + p_{2022}$ jika dibagi 16 adalah $\boxed{9}$.

Contoh 3.2 (Bulgaria 1996/#7)

Tentukan semua pasangan bilangan prima (p, q) sehingga $pq \mid (5^p - 2^p)(5^q - 2^q)$.

Perhatikan bahwa (p, q) solusi maka (q, p) juga solusi. W.L.O.G. $p \leq q$. Karena $pq \mid (5^p - 2^p)(5^q - 2^q)$, maka

$$p \mid (5^p - 2^p)(5^q - 2^q).$$

Jika $p \mid 5^p - 2^p$, dari **Fermat Little Theorem (Teorema 3.3)**, maka

$$5^p - 2^p \equiv 5 - 2 \equiv 3 \pmod{p} \implies p \mid 3.$$

Maka $p = 3$. Subtitusikan, maka

$$3q \mid \left(5^3 - 2^3\right)(5^q - 2^q) \implies q \mid 39\,(5^q - 2^q).$$

Jika $q \mid 5^q - 2^q$, dengan cara yang sama diperoleh $q = 3$. Maka $(p, q) = (3, 3)$. Jika $q \nmid 5^q - 2^q$, maka $q \mid 39$ dan diperoleh $q = 13$. Maka $(p, q) = (3, 13)$. Jika $p \nmid 5^p - 2^p$, maka $p \mid 5^q - 2^q$. Cukup jelas bahwa $p = 2$ dan $p = 5$ bukan solusi yang berarti $\gcd(p, 2) = \gcd(p, 5) = 1$. Kita punya

$$5^q \equiv 2^q \pmod{p} \iff \left(\frac{5}{2}\right)^q \equiv 1 \pmod{p}.$$

Misalkan $x \equiv \frac{1}{2} \pmod{p}$, yaitu menyatakan invers dari $2 \pmod{p}$. Maka $(5x)^q \equiv 1 \pmod{p}$ dan dari **Teorema 1.1** berlaku $\mathrm{ord}_p(5x) \mid q$. Maka $\mathrm{ord}_p(5x) \in \{1, q\}$.

- Jika $\mathrm{ord}_p(5x) = 1$, maka $5x \equiv 1 \pmod{p}$ yang berarti

  $$\frac{5}{2} \equiv 1 \pmod{p} \iff 5 \equiv 2 \pmod{p} \iff 3 \equiv 0 \pmod{p}.$$

  Maka $p \mid 3 \iff p = 3$. Kontradiksi bahwa $p \nmid 5^p - 2^p$.
- Jika $\mathrm{ord}_p(5x) = q$, dari **Lemma 1.3**, maka $\mathrm{ord}_p(5x) \mid \varphi(p) \implies q \mid p - 1 \implies q \leq p - 1 \leq q - 1$ yang jelas kontradiksi.

Sehingga solusinya adalah $\boxed{(p, q) = (3, 3), (3, 13), (13, 3)}$.

Teorema 3.3 (Fermat Little Theorem)

Jika a bilangan bulat dan p bilangan prima serta $\gcd(a, p) = 1$, maka $a^{p-1} \equiv 1 \pmod{p}$.

Contoh 3.4

Tentukan semua bilangan asli sehingga $2^{n-1} + 1$ habis dibagi n.

Kita klaim bahwa $n = 1$ merupakan satu-satunya solusi. Andaikan ada $n > 1$ yang memenuhi, maka n haruslah ganjil. Misalkan $n = 2^k m + 1$ di mana m bilangan ganjil dan p adalah sembarang faktor prima ganjil dari n. Maka

$$p \mid n \mid 2^{n-1} - 1 = 2^{2^k m} + 1 \implies p \mid 2^{2^k m} + 1.$$

Kita punya

$$2^{2^k m} \equiv -1 \pmod{p} \implies 2^{2^{k+1} m} \equiv 1 \pmod{p} \iff \mathrm{ord}_p(2) \mid 2^{k+1} m.$$

Dari **Teorema 1.1**, haruslah $\mathrm{ord}_p(2) \nmid 2^k m$. Maka haruslah $\mathrm{ord}_p(2) = 2^{k+1} t$ untuk suatu bilangan asli t yang memenuhi $t \mid m$. Dari **Lemma 1.3**, maka

$$\mathrm{ord}_p(2) \mid \varphi(p) = p - 1 \implies 2^{k+1} t \mid p - 1 \implies 2^{k+1} \mid p - 1.$$

Maka $p \equiv 1 \pmod{2^{k+1}}$ untuk sembarang faktor prima dari n. Kita punya

$$n = \prod_{\substack{p|n \\ a_i \in \mathbb{N}}} p^{a_i} \equiv \prod_{\substack{p|n \\ a_i \in \mathbb{N}}} 1^{a_i} \equiv 1 \pmod{2^{k+1}} \implies n \equiv 1 \pmod{2^{k+1}}.$$

Maka $2^{k+1} \mid n-1 = 2^k m \implies 2^{k+1} \mid 2^k m$ yang jelas kontradiksi. Jadi, untuk $n > 1$ tidak ada solusi.

> **Remark.** Seringkali penyelesaian yang terkait dengan order akan melibatkan suatu bilangan prima. Sehingga untuk tipe soal seperti di atas bisa meninjau sebarang prima atau prima terkecil dari n.

Contoh 3.5 (OSN 2013/#6)

Suatu bilangan asli n dikatakan *kekar* jika terdapat bilangan asli x sedemikian sheingga $x^{nx} + 1$ habis dibagi 2^n.

(a). Buktikan bahwa 2013 bilangan kekar.

(b). Jika m bilangan kekar, tentukan bilangan asli y terkecil (dalam m) sehingga $y^{my} + 1$ habis dibagi 2^m.

Kita bisa simpulkan bahwa $2^n \mid x^{nx} + 1$ terpenuhi ketika x ganjil.

(a). Tinjau $x = 2^{2013} - 1$ memenuhi karena

$$x^{2013x} \equiv (-1)^{2013\left(2^{2013}-1\right)} \equiv -1 \pmod{2^{2013}} \implies 2013 \mid x^{2013x} + 1$$

yang berarti menunjukkan 2013 kekar.

> **Remark.** Sebenarnya kita tinggal menemukan x sehingga $x^{2013x} \equiv -1 \pmod{2^{2013}}$. Kita juga tahu $2013x$ ganjil. Kita bisa tuliskan juga $x^{2013x} \equiv (-1)^{2013x} \pmod{2^{2013}}$. Dengan asumsi $x \equiv -1 \pmod{2^{2013}}$, kita mudah mengecek $x = 2^{2013} - 1$ adalah solusi.

(b). Jawabannya adalah $y = 2^m - 1$. Jika m genap, misalkan $m = 2k$, maka

$$y^{my} + 1 = \left(y^{ky}\right)^2 + 1 \equiv 1 + 1 \equiv 2 \pmod{4}.$$

Karena $2^m \mid y^{my} + 1$, haruslah $m = 1$ yang mana kontradiksi. Jadi, m ganjil. Jika $m = 1$, kita peroleh $2 \mid y^m + 1$ yang mana $y = 1$ terpenuhi. Sekarang tinjau untuk $m > 1$. Misalkan $\text{ord}_{2^m}(y) = s$. Perhatikan bahwa

$$y^{my} \equiv -1 \pmod{2^m} \implies y^{2my} \equiv 1 \pmod{2^m}.$$

Dari **Teorema 1.1**, maka $s \mid 2my$. Dari **Lemma 1.3**, maka $s \mid \varphi(2^m) \implies s \mid 2^{m-1}$. Maka $s \mid \gcd\left(2my, 2^{m-1}\right) = 2\gcd\left(my, 2^{m-2}\right)$. Karena my ganjil, kita punya $s \mid 2$. Kita peroleh $y^2 \equiv 1 \pmod{2^m}$. Kita punya

$$0 \equiv y^{my} + 1 \equiv \left(y^2\right)^{\frac{my-1}{2}} \cdot y + 1 \equiv 1^{\frac{my-1}{2}} \cdot y + 1 \equiv y + 1 \pmod{2^m}.$$

Maka $2^m \mid y + 1$ dan bilangan asli y terkecil yang memenuhi adalah $y = 2^m - 1$.

§4 Latihan Soal

Tidak semua soal berikut harus diselesaikan dengan konsep order. Anda dapat menggunakan metode lain atau gabungan dari metode lain dengan konsep order. Bisa jadi urutan soal berikut tidak urut sesuai tingkat kesulitan. Soal yang tersedia solusinya berlabel $\star$.

Problem 4.1. Diberikan bilangan bulat a, x, y dan b bilangan asli di mana $\gcd(a, b) = 1$. Buktikan bahwa $a^x \equiv a^y \pmod{b}$ jika dan hanya jika $\mathrm{ord}_b(a) \mid x - y$.

Problem 4.2. Buktikan $\mathrm{ord}_{101}(2) = 100$.

Problem 4.3. Jika a bilangan asli yang lebih besar dari 1 dan n bilangan asli, buktikan $n \mid \varphi(a^n - 1)$.

Problem 4.4. Buktikan setiap faktor prima dari $2^p - 1$ lebih besar dari p untuk suatu bilangan prima p.

Problem 4.5 (Kazakhstan 2000/#5)**.** Misalkan p bilangan prima merupakan pembagi dari $2^{2^k} + 1$. Buktikan bahwa $p - 1$ habis dibagi 2^{k+1}. $\star$

Problem 4.6 (Euler)**.** Buktikan bahwa semua faktor positif $2^{2^n} + 1$ berbentuk $2^{n+1}k + 1$ di mana k bilangan bulat tak negatif.

Problem 4.7. Jika g adalah akar primitif dari bilangan prima ganjil p, buktikan bahwa

$$g^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Problem 4.8. Jika r adalah akar primitif modulo m, maka inverse dari r modulo m juga akar primitif.

Problem 4.9 (Wolstenholme's)**.** *Untuk bilangan prima $p > 3$, maka*

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{(p-1)^2} \equiv 0 \pmod{p}.$$

Problem 4.10 (Wilson)**.** *Jika p bilangan prima, buktikan bahwa* $(p-1)! \equiv -1 \pmod{p}$.

Problem 4.11. Jika p bilangan prima dan $p \mid a^2 + b^2$ di mana a, b bilangan bulat yang relatif prima dengan p, buktikan $p \equiv 1 \pmod{4}$.

Problem 4.12. Diberikan bilangan prima ganjil p. Jika q dan r dua bilangan prima sedemikian sehingga $p \mid q^r + 1$, buktikan bahwa $2r \mid p - 1$ atau $p \mid q^2 - 1$.

Problem 4.13. Buktikan terdapat faktor prima $p^p - 1$ yang berbentuk $kp + 1$ untuk suatu bilangan prima p dan k bilangan asli.

Problem 4.14. *Jika a, b adalah dua bilangan bulat yang relatif prima dengan m, serta dua bilangan asli x, y memenuhi* $a^x \equiv b^x \pmod{m}$ *dan* $a^y \equiv b^y \pmod{m}$*. Buktikan bahwa*

$$a^{\gcd(x,y)} \equiv b^{\gcd(x,y)} \pmod{m}.$$

Problem 4.15 (Opsilon 2022)**.** Tentukan semua bilangan prima p sedemikian sehingga

$$1^{p-2} + 2^{p-2} + 3^{p-2} + \cdots + p^{p-2}$$

bilangan prima.

Problem 4.16. Diberikan a, b bilangan asli dan $\gcd(a, b) = 1$. Buktikan pembagi ganjil dari $a^{2^n} + b^{2^n}$ berbentuk $2^{n+1}m + 1$ untuk setiap bilangan asli n dan suatu bilangan asli m.

Problem 4.17 (AIME 2019/#14)**.** Tentukan bilangan prima ganjil terkecil dari $2019^8 + 1$.

Problem 4.18. Buktikan untuk sembarang bilangan asli a, maka $a^{2^n}+1$ tidak memiliki faktor bilangan asli di interval $\left[3, 2^{n-1}\right]$ untuk setiap bilangan asli $n > 2$.

Problem 4.19 (Fermat)**.** Misalkan $p > 3$ bilangan prima. Buktikan bahwa sembarang faktor positif dari $\frac{2^p+1}{3}$ berbentuk $2kp+1$ untuk suatu bilangan bulat k. ⋆

Problem 4.20. Tentukan semua bilangan asli n sehingga $2^n - 1$ habis dibagi n.

Problem 4.21. Tentukan semua bilangan asli n sehingga $n^2 \mid 3^n + 1$.

Problem 4.22 (Wolstenholme's)**.** *Untuk setiap prima $p \geq 5$, buktikan bahwa $\binom{2p-1}{p-1} - 1$ habis dibagi p^3.* ⋆

Problem 4.23. Buktikan bahwa $\binom{2p}{p} - 2$ habis dibagi p^2 untuk setiap prima $p > 2$.

Problem 4.24 (Romania TST 2019/#1)**.** Misalkan bilangan asli $k \geq 2$ dan bilangan asli $n_1, n_2, \cdots, n_k \geq 1$ memenuhi

$$n_2 \mid 2^{n_1} - 1, \quad n_3 \mid 2^{n_2} - 1, \quad \cdots, \quad n_k \mid 2^{n_{k-1}} - 1, \quad n_1 \mid 2^{n_k} - 1.$$

Buktikan bahwa $n_1 = n_2 = \cdots = n_k = 1$. ⋆

Problem 4.25. Jika $n > 1$ bilangan asli sehingga $3^n + 4^n$ habis dibagi n, buktikan n habis dibagi 7.

Problem 4.26 (Wildan Bagus W.)**.** Tentukan banyak bilangan asli $n \leq 2022$ yang memenuhi

$$\gcd\left(2021^{2^n}+1, n\right) = 1.$$

Problem 4.27 (USA TST 2003)**.** Tentukan semua tripel bilangan prima (p, q, r) yang memenuhi

$$p \mid q^r + 1, \quad q \mid r^p + 1, \quad r \mid p^q + 1.$$

⋆

Problem 4.28 (Romania TST 1996/#3)**.** Tentukan semua bilangan prima p dan q sehingga untuk setiap bilangan asli n berlaku $n^{3pq} - n$ habis dibagi $3pq$. ⋆

Problem 4.29 (China TST 2006)**.** Tentukan semua bilangan asli a dan n sehingga

$$\frac{(a+1)^n - a^n}{n}$$

bilangan bulat.

Problem 4.30. Untuk sembarang bilangan ganjil n, buktikan bahwa tidak terdapat bilangan bulat m sehingga $m^{n-1} + 1$ kelipatan n.

Problem 4.31 (South Korean 2007/#4)**.** Tentukan semua pasangan bilangan prima (p, q) sehingga $p^p + q^q + 1$ habis dibagi pq.

Problem 4.32 (APMO 2006/#3)**.** Misalkan $p \geq 5$ bilangan prima dan r menyatakan banyak cara meletakkan p dam pada papan $p \times p$ sehingga tidak semua dam berada di satu baris (tapi mereka semua bisa dalam satu kolom). Buktikan bahwa r habis dibagi p^5. Asumsikan bahwa semua dam identik.

Problem 4.33 (Wildan Bagus W.)**.** Tentukan semua bilangan prima ganjil p sehingga

$$1^{p^2-p-5} + 2^{p^2-p-5} + 3^{p^2-p-5} + \cdots + p^{p^2-p-5}$$

habis dibagi p^2.

Problem 4.34 (Bulgaria 2016/#1)**.** Tentukan semua bilangan asli m dan n sehingga $\left(2^{2^m}+1\right)\left(2^{2^n}+1\right)$ habis dibagi mn.

Problem 4.35 (Iran MO 2016 Round 3/#P1)**.** Misalkan p dan q dua bilangan prima di mana q ganjil. Buktikan bahwa terdapat bilangan bulat x sehingga

$$q \mid (x+1)^p - x^p$$

jika dan hanya jika $q \equiv 1 \pmod{p}$.

Problem 4.36 (HMMT November 2014/#10)**.** Misalkan m dan n bilangan bulat di mana $1 \leq m \leq 49$ dan $n \geq 0$ sehingga m membagi $n^{n+1} + 1$. Tentukan banyak kemungkinan nilai m.

Problem 4.37 (CWMO 2015/#8)**.** Misalkan k bilangan asli dan $n = \left(2^k\right)!$. Buktikan $\sigma(n)$ memiliki faktor prima yang lebih besar dari 2^k, di mana $\sigma(n)$ menyatakan jumlah semua faktor positif dari n. ⋆

Problem 4.38 (APMO 2012/#3)**.** Tentukan semua pasangan (p, n) di mana p bilangan prima dan n bilangan asli sehingga $\frac{n^p+1}{p^n+1}$ bilangan bulat.

Problem 4.39 (China 2009/#2)**.** Tentukan semua bilangan prima p, q sehingga $5^p + 5^q$ habis dibagi pq.

Problem 4.40 (USA TST EGMO 2019/#3)**.** Misalkan n bilangan asli sehingga

$$\frac{1^k + 2^k + \cdots + n^k}{n}$$

untuk sembarang $k \in \{1, 2, \cdots, 99\}$. Buktikan bahwa n tidak memiliki pembagi di antara 2 dan 100, inklusif.

§5 Petunjuk

4.1. Cukup mudah :)

4.2. Tinjau faktor dari 100: $1, 2, 4, 5, 10, 20, 25, 50, 100$. Anda harus membuktikan bahwa untuk $a^x \not\equiv 1 \pmod{101}$ untuk $x \neq 100$. Anda tidak perlu mencoba semua kemungkinan, bagaimana Anda mengatasi hal tersebut?

4.3. Tentukan $\text{ord}_a\,(a^n - 1)$.

4.4. Misalkan q adalah faktor prima $2^p - 1$. Tentukan $\text{ord}_q(2)$.

4.5. Tinjau $2^{2^k} \equiv -1 \pmod{p} \implies 2^{2^{k+1}} \equiv 1 \pmod{p}$. Tentukan $\text{ord}_p(2)$.

4.6. Buktikan bahwa untuk sembarang faktor prima dari $2^{2^n} + 1$ berbentuk $1 \pmod{2^{n+1}}$.

4.7. Cukup pakai definisi akar primitif.

4.8. Misalkan invers $r \pmod{m}$ adalah x. Gunakan definisi invers dan kondisi akar primitif.

4.9. Cukup mudah dengan suatu lemma.

4.10. Misalkan g adalah akar primitif modulo p dan **Teorema 2.5**.

4.11. Tinjau $a^2 \equiv -b^2 \pmod{p} \iff (a \cdot b^{-1})^2 \equiv -1 \pmod{p}$. Tentukan $\text{ord}_p\left(a \cdot b^{-1}\right)$.

4.12. Tinjau $q^r \equiv -1 \pmod{p} \implies q^{2r} \equiv 1 \pmod{p}$. Tentukan semua kemungkinan $\text{ord}_p(q)$.

4.13. **Lemma 1.3**.

4.14. Tinjau $\left(a \cdot b^{-1}\right)^x \equiv 1 \pmod{m}$ dan $\left(a \cdot b^{-1}\right)^y \equiv 1 \pmod{m}$. Gunakan **Theorem 1.1**.

4.15. Tinjau $\mod p$.

4.16. Buktikan setiap faktor prima ganjil dari $a^{2^n} + b^{2^n}$ berbentuk $1 \pmod{2^{n+1}}$.

4.17. **Lemma 1.3**.

4.18. Andaikan ada $d \in \left[3, 2^{n-1}\right]$ sehingga $d \mid a^{2^n} + 1$. Tentukan interval faktor prima dari d.

4.19. Tunjukkan bahwa $\gcd\left(\frac{2^p+1}{3}, 3\right) = 1$ dan tinjau sembarang faktor prima dari $\frac{2^p+1}{3}$.

4.20. Untuk $n > 1$, tinjau faktor prima terkecil n dan **Lemma 1.3**.

4.21. Untuk $n > 1$, tinjau faktor prima terkecil n.

4.22. $\binom{2p-1}{p-1} = \frac{2p-1}{p-1} \cdot \frac{2p-2}{p-2} \cdot \ldots \cdot \frac{p+1}{1} = \prod_{i=1}^{p-1} \left(1 + \frac{p}{i}\right)$ dan bongkar.

4.23. Cari bentuk yang ekuivalen dengan $\binom{2p}{p}$.

4.24. Jika $a, b \in \mathbb{N}$ dan $x > 1$, buktikan $x^a - 1 \mid x^b - 1 \iff a \mid b$. Misalkan pula $s = \text{KPK}(n_1, n_2, \cdots, n_k)$ dan gunakan keterbagian pada soal.

4.25. Tinjau faktor prima terkecil dari n.

4.26. Buktikan tidak ada faktor prima dari n yang membagi 2021^{2^n} jika n genap.

4.27. Bagi kasus jika ada dari p, q, r yang genap dan ketika semuanya ganjil. Cukup pakai **Teorema 1.1** dan **Lemma 1.3**.

4.28. Buktikan $p \neq q \neq 3 \neq p$. Pilih n sebagai akar primitif modulo p dan modulo q.

4.29. Tinjau faktor prima terkecil dari n, katakan p, dan tentukan $\text{ord}_p\left((a+1)\cdot a^{-1}\right)$.

4.30. **Contoh 3.4**.

4.31. Tinjau mod p dan mod q.

4.32. $r = \binom{p^2}{p} - p$ dan **Teorema 2.7**.

4.33. $\varphi\left(p^2\right) = p^2 - p$ dan kita peroleh $i^{p^2-p-5} \equiv \frac{1}{i^5} \pmod{p^2}$ untuk $\gcd(i,p) = 1$. Metodenya mirip dengan pembuktian **Teorema 2.7**.

4.34. Tinjau ketika ada prima p sehingga $p \mid 2^{2^t} + 1$.

4.35. Pembuktian dari kiri ke kanan cukup memakai **Teorema 1.1** dan **Lemma 1.3**. Pembuktian dari kanan ke kiri, tinjau akar primitif mod q.

4.36. Buktikan bahwa semua bilangan m ganjil, ada n sehingga $m \mid n^{n+1} + 1$. Selainnya, gunakan lemma: buktikan bahwa jika p prima ganjil, maka $p \mid n^2 + 1$ jika dan hanya jika $p \equiv 1 \pmod 4$.

4.37. Tentukan $\nu_2(n)$, yaitu bilangan bulat terbesar l sehingga $2^l \mid n$. Buktikan bahwa $2^{2^{k-1}} + 1 \mid \sigma(n)$.

4.38. Bagi kasus $p = 2$ dan $p \geq 3$. Untuk $p \geq 3$, buktikan $p+1 \mid n^p + 1$ dan tentukan $\text{ord}_{p+1}(n)$. *Bounding.*

4.39. Bagi kasus. Untuk $p, q \neq 5$, buktikan $\nu_2\left(\text{ord}_q(5)\right) = 1 + \nu_2(p-1)$ dan $\nu_2\left(\text{ord}_p(5)\right) = 1 + \nu_2(q-1)$. Untuk $p \neq q$, buktikan $\nu_2(\text{ord}_q(5)) = 1 + \nu_2(|p-q|)$.

4.40. Andaikan ada $2 \leq p \leq 100$ sehingga $p \mid n$. Misalkan $S_k = 1^k + 2^k + \cdots + n^k$. Bagaimana lota menemukan formula dari S_k? Tidak perlu mencari bentuk eksplisit dari S_k (kita tahu bagaimana untuk $k \geq 4$), melainkan kita bisa menemukan bentuk teleskopiknya.

§6 Solusi Soal Terpilih

4.5. Perhatikan bahwa

$$2^{2^k} \equiv -1 \pmod{p} \implies 2^{2^{k+1}} \equiv 1 \pmod{p}.$$

Dari **Teorema 1.1**, maka $\text{ord}_p(2) \mid 2^{k+1}$. Karena $2^{2^k} \not\equiv 1 \pmod{p}$, dari **Teorema 1.1** berlaku $\text{ord}_p(2) \nmid 2^k$. Jadi, $\text{ord}_p(2) = 2^{k+1}$. Dari **Lemma 1.3**, maka

$$\text{ord}_p(2) \mid \varphi(p) \implies 2^{k+1} \mid p-1$$

seperti yang ingin dibuktikan. ■

4.19. Kita klaim bahwa $\gcd\left(\frac{2^p+1}{3}, 3\right) = 1$. Hal ini ekuivalen dengan menunjukkan $9 \nmid 2^p + 1$. Dari **Teorema 1.4**, kita punya

$$2^{\varphi(9)} \equiv 1 \pmod{9} \implies 2^6 \equiv 1 \pmod{9}.$$

Karena $p \equiv 1, 5 \pmod{6}$, maka

$$2^p + 1 \equiv 2^{p \pmod 6} + 1 \equiv 3 \pmod{9} \implies 9 \nmid 2^p + 1.$$

Misalkan q adalah sembarang faktor prima dari $\frac{2^p+1}{3}$. Maka

$$q \mid \frac{2^p+1}{3} \mid 2^p + 1 \implies q \mid 2^p + 1 \iff 2^p \equiv -1 \pmod{q} \implies 2^{2p} \equiv 1 \pmod{q}.$$

Dari **Teorema 1.1**, maka $\text{ord}_q(2) \mid 2p$ dan $\text{ord}_q(2) \nmid p$. Kita peroleh $\text{ord}_q(2) = 2$ atau $\text{ord}_q(2) = 2p$. Jika $\text{ord}_q(2) = 2 \implies q \mid 2^2 - 1 = 3$, maka kontradiksi. Sehingga $\text{ord}_q(2) = 2p$ dan dari **Lemma 1.3**, kita punya $\text{ord}_q(2) \mid \varphi(q) = q - 1 \implies 2p \mid q - 1$. Maka $q \equiv 1 \pmod{2p}$. Faktor positif lain diperoleh dari perkalian beberapa bilangan prima yang berbentuk $1 \pmod{2p}$, sehingga faktor positif tersebut juga akan berbentuk $1 \pmod{2p}$ (lihat **Contoh 3.4**). Terbukti bahwa sembarang faktor positif dari $\frac{2^p+1}{3}$ berbentuk $2kp + 1$ atau $1 \pmod{2p}$. ■

4.22. Tinjau

$$\binom{2p-1}{p-1} = \frac{(2p-1)(2p-2)\cdots(p+1)p!}{p!(p-1)!} = \frac{2p-1}{p-1} \cdot \frac{2p-2}{p-2} \cdot \ldots \cdot \frac{p+1}{1}$$

yang ekuivalen dengan

$$\binom{2p-1}{p-1} = \left(1 + \frac{p}{p-1}\right)\left(1 + \frac{p}{p-2}\right)\cdots\left(1 + \frac{p}{1}\right).$$

Pandang polinomial

$$\begin{aligned} P(x) &\equiv \left(1 + \frac{x}{p-1}\right)\left(1 + \frac{x}{p-2}\right)\cdots\left(1 + \frac{x}{1}\right) \pmod{p^3} \\ &\equiv 1 + x\sum_{i=1}^{p-1}\frac{1}{i} + x^2 \sum_{1\le i<j\le p-1}\frac{1}{ij} + x^3 \sum_{1\le i<j<k\le p-1}\frac{1}{ijk} + \cdots + x^{p-1}\cdot\frac{1}{(p-1)!} \pmod{p^3}. \end{aligned}$$

Maka

$$P(p) \equiv 1 + p\sum_{i=1}^{p-1}\frac{1}{i} + p^2 \sum_{1\le i<j\le p-1}\frac{1}{ij} \pmod{p^3}.$$

Dari **Teorema 2.7**, kita punya $\sum_{i=1}^{p-1}\frac{1}{i} \equiv 0 \pmod{p^2} \implies p\sum_{i=1}^{p-1}\frac{1}{i} \equiv 0 \pmod{p^3}$. Dari **Teorema 2.7** dan **Problem 4.9**, maka

$$\sum_{1\le i<j\le p-1}\frac{1}{ij} = \frac{1}{2}\left(\sum_{i=1}^{p-1}\frac{1}{i}\right)^2 - \frac{1}{2}\sum_{i=1}^{p-1}\frac{1}{i^2} \equiv 0 \pmod{p} \implies p^2 \sum_{1\le i<j\le p-1}\frac{1}{ij} \equiv 0 \pmod{p^3}.$$

Maka

$$\binom{2p-1}{p-1} \equiv P(p) \equiv 1 + 0 + 0 \equiv 1 \pmod{p^3} \implies \binom{2p-1}{p-1} \equiv 1 \pmod{p^3}$$

seperti yang ingin dibuktikan. ■

4.24. Pembuktian $x^a - 1 \mid x^b - 1 \iff a \mid b$ diserahkan kepada pembaca sebagai latihan. Jika ada $1 \leq i \leq k$ sehingga $n_i = 1$, maka $n_{i-1} \mid 2^{n_i} - 1 = 1$, sehingga $n_{i-1} = 1$. Akibatnya, $n_1 = n_2 = \cdots = n_k = 1$. Tinjau ketika $n_1, n_2, \cdots, n_k > 1$. Misalkan $s = \text{KPK}(n_1, n_2, \cdots, n_k)$. Maka $2^{n_i} - 1 \mid 2^s - 1$ untuk setiap $1 \leq i \leq k$. Kita punya

$$n_{i-1} \mid 2^{n_i} - 1 \mid 2^s - 1 \implies n_{i-1} \mid 2^s - 1 \; \forall \; 1 \leq i \leq k, n_0 = n_k.$$

Maka $\text{KPK}(n_1, n_2, \cdots, n_k) \mid 2^s - 1 \implies s \mid 2^s - 1$. Misalkan p faktor prima terkecil dari s. Maka $p \mid s \mid 2^s - 1 \implies p \mid 2^s - 1$. Dari **Teorema 1.1**, maka $\text{ord}_p(2) \mid s$. Dari **Lemma 1.3**, maka $\text{ord}_p(2) \mid p - 1$. Kita punya $\text{ord}_p(2) \mid \gcd(s, p-1)$. Andaikan $\gcd(s, p-1) = d > 1$, maka ada faktor prima dari d, katakan q, sehingga $q \mid s$ dan $q \mid p-1$. Jelas $q < p$, sehingga s memiliki faktor prima yang lebih kecil dari p, kontradiksi. Jadi, $\gcd(s, p-1) = 1$ dan kita punya $\text{ord}_p(2) \mid 1 \iff \text{ord}_p(2) = 1 \iff 2^1 \equiv 1 \pmod{p} \iff p \mid 1$. Kontradiksi. Maka tidak ada solusi untuk kasus ini. ■

4.27. Jawabannya adalah $(p, q, r) = (2, 5, 3), (3, 2, 5), (5, 3, 2)$. Tinjau bahwa jika (p, q, r) solusi, maka permutasi siklis (p, q, r) juga solusi. Jika ada dari p, q, r yang bernilai 2, W.L.O.G. $p = 2$. Kita punya $2 \mid q^r + 1, q \mid r^2 + 1$, dan $r \mid 2^q + 1$ sehiingga q, r ganjil. Tinjau

$$2^q \equiv -1 \pmod{r} \implies 2^{2q} \equiv 1 \pmod{r}.$$

Dari **Teorema 1.1**, maka $\text{ord}_r(2) \mid 2q$ dan $\text{ord}_r(2) \nmid q$. Maka $\text{ord}_r(2) \in \{2, 2q\}$.

- Jika $\text{ord}_r(2) = 2$, maka $2^2 \equiv 1 \pmod{4} \iff r \mid 3$. Maka $r = 3$ dan diperoleh $q \mid 3^2 + 1 = 10 \implies q = 5$. Cek $(p, q, r) = (2, 5, 3)$,

  $$2 \mid 5^3 + 1 = 126, \quad 5 \mid 3^2 + 1 = 10, \quad 3 \mid 2^5 + 1 = 33$$

  yang mana memenuhi. Jadi, $(p, q, r) = (2, 5, 3), (3, 2, 5), (5, 3, 2)$ merupakan solusi.
- Jika $\text{ord}_r(2) = 2q$, dari **Lemma 1.3**, maka $2q \mid \varphi(r) = r - 1 \implies q \mid r - 1 \iff r \equiv 1 \pmod{q}$. Maka

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

  Sehingga haruslah $q \mid 2 \implies q = 2$, kontradiksi q ganjil.

Jika $p, q, r \geq 3$. Seperti sebelumnya, kita peroleh

$$\text{ord}_p(q) \in \{2, 2r\}, \quad \text{ord}_q(r) \in \{2, 2p\}, \quad \text{ord}_r(p) \in \{2, 2q\}.$$

Jika $\text{ord}_p(q) = 2r$, dari **Lemma 1.3** dan kita peroleh $2r \mid q - 1 \implies q \equiv 1 \pmod{r}$. Maka

$$0 \equiv r^p + 1 \equiv 1^p + 1 \equiv 2 \pmod{q} \implies q \mid 2.$$

Kontradiksi. Begitu juga jika $\text{ord}_q(r) = 2p$ atau $\text{ord}_r(p) = 2q$ akan diperoleh kontradiksi. Maka $\text{ord}_p(q) = \text{ord}_q(r) = \text{ord}_r(p) = 2$ sehingga

$$q^2 \equiv 1 \pmod{p} \iff (q+1)(q-1) \equiv 0 \pmod{p} \implies q \equiv -1 \pmod{p}.$$

Secara analog, diperoleh $r \equiv -1 \pmod{q}$ dan $p \equiv -1 \pmod{r}$. Maka $p \mid q + 1, q \mid r + 1$, dan $r \mid p + 1$. Kita punya $p \leq q + 1, q \leq r + 1$, dan $r \leq p + 1$ sehingga diperoleh

$$p \leq q + 1 \leq r + 2 \leq p + 3.$$

Maka $q \in \{p - 1, p, p + 1, p + 2\}$. Misalkan $q = p + x$ di mana $x \in \{-1, 0, 1, 2\}$. Maka

$$p \mid q + 1 = p + x + 1 \implies p \mid x + 1.$$

Kita peroleh $x = -1$ atau $x = 2$. Jika $x = 2$, maka $p \mid 3 \iff p = 3$. Maka $q = 5$ dan diperoleh $r \mid 4 \implies r = 2$, kontradiksi. Jika $x = -1$, misalkan pula $r = p + y$ di mana $y \in \{-2, -1, 0, 1\}$. Maka

$$q \mid r + 1 = p + y \implies p - 1 \mid p + y \implies p - 1 \mid y + 1.$$

Jika $y = -2$ atau $y = 0$ diperoleh $p = 2$, kontradiksi. Jika $y = 1$, diperoleh $p = 3$. Maka $q = 2$, kontradiksi. Jika $y = -1$, dari $r \mid p + 1$ diperoleh

$$p - 1 \mid p + 1 \implies p - 1 \mid p + 1 - (p - 1) = 2 \implies p = 3.$$

Maka $r = 2$, kontradiksi. Sehingga tidak ada solusi lain.

4.28. Jawabannya adalah $(p, q) = (11, 7), (7, 11)$. Kita klaim bahwa $3, p, q$ harus saling berbeda. Andaikan ada yang sama, misalkan A dan B (dua dari $3, p$, dan q), maka $A^2 \mid n^{A^2c} - n$. Ambil $n = A$, maka $A^2 \mid A^{A^2c} - A$ sehingga $A^2 \mid A$, kontradiksi. W.L.O.G. $p > q$. Jika $q = 2$, maka $6p \mid n^{6p} - n \implies 3 \mid n^{6p} - n$. Dari **Teorema 3.3**, untuk $\gcd(n, 3) = 1$ berlaku $n^2 \equiv 1 \pmod 3$ sehingga $n^{6p} \equiv \left(n^2\right)^{3p} \equiv 1 \pmod 3$. Maka

$$0 \equiv n^{6p} - n \equiv 1 - n \pmod 3 \implies n \equiv 1 \pmod 3,$$

sehingga tidak berlaku untuk $n \equiv 2 \pmod 3$ yang mana kontradiksi berlaku untuk setiap $n \in \mathbb{N}$. Jadi, $3 < q < p$. Misalkan P akar primitif modulo p. Kita punya $\gcd(p, P) = 1$. Maka $\text{ord}_p(P) = p - 1$ dan tinjau untuk $n = P$,

$$3pq \mid P^{3pq} - P \implies p \mid P^{3pq} - P = P\left(P^{3pq-1} - 1\right) \implies p \mid P^{3pq-1} - 1.$$

Karena $P^{p-1} \equiv 1 \pmod p$, kita peroleh

$$1 \equiv P^{3pq-1} \equiv P^{3pq-1 \pmod{p-1}} \equiv P^{3q-1} \pmod p.$$

Dari **Teorema 1.1**, kita punya $p - 1 \mid 3q - 1$. Secara analog, kita peroleh juga $q - 1 \mid 3p - 1$. Misalkan pula $3p - 1 = (q - 1)x$ dan $3q - 1 = (p - 1)y$ di mana $x, y \in \mathbb{N}$. Andaikan $y \geq 4$, maka

$$3q - 1 \geq 4(p - 1) > 4(q - 1) \implies 3q - 1 > 4q - 4 \iff 3 > q$$

Kontradiksi. Maka $y \leq 3$. Jika $y = 3$, kita punya

$$3q - 1 = 3(p - 1) = 3p - 3 \implies 3(p - q) = 2,$$

tidak ada solusi. Jika $y = 2$, kita punya

$$3q - 1 = 2(p - 1) = 2p - 2 \implies p = \frac{3q + 1}{2}.$$

Tinjau bahwa $q = \frac{3p-1}{x} + 1 = \frac{3p+x-1}{x}$. Maka

$$p = \frac{3q + 1}{2} = \frac{9p + 3x - 3 + x}{2x} = \frac{9p + 4x - 3}{2x}.$$

Kita punya

$$2xp = 9p + 4x - 3 \iff p(2x - 9) = 4x - 3 \iff p = \frac{4x - 3}{2x - 9} = 2 + \frac{15}{2x - 9}.$$

Maka $2x - 9 \mid 15$ dan diperoleh $\frac{15}{2x-9} \in \{1, 3, 5, 15\}$. Karena p prima, diperoleh $p \in \{7, 17\}$. Subtitusikan ke $p = \frac{3q+1}{2}$ dipenuhi oleh $p = 17$ sehingga $q = 11$. Maka $(p, q) = (17, 11), (11, 17)$ adalah solusi. Jika $y = 1$, maka

$$3q - 1 = p - 1 \iff p = 3q,$$

sehingga kontradiksi p prima. Jadi, tidak ada solusi lain.

4.37. Tinjau bahwa

$$\nu_2(n) = \sum_{i\geq 1} \left\lfloor \frac{2^k}{2^i} \right\rfloor = 2^{k-1} + 2^{k-2} + \cdots + 1 = 2^k - 1.$$

Misalkan faktorisasi prima $n = 2^{2^k-1} p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$ di mana $p_i \geq 3$ untuk setiap $1 \leq i \leq t$. Maka

$$\sigma(n) = \frac{2^{2^k-1+1}-1}{2-1} \prod_{i=1}^{t} \frac{p_i^{a_i+1}-1}{p_i-1} = \left(2^{2^k}-1\right) \prod_{i=1}^{t} \frac{p_i^{a_i+1}-1}{p_i-1}.$$

Maka $2^{2^k}-1 \mid \sigma(n)$. Tinjau $2^{2^k}-1 = \left(2^{2^{k-1}}+1\right)\left(2^{2^{k-1}}-1\right)$, kita punya $2^{2^{k-1}}+1 \mid \sigma(n)$. Tinjau prima p sehingga $p \mid 2^{2^{k-1}}+1$, kita punya juga $p \mid \sigma(n)$. Maka

$$2^{2^{k-1}} \equiv -1 \pmod{p} \implies 2^{2^k} \equiv 1 \pmod{p}.$$

Dari **Teorema 1.1**, maka $\text{ord}_p(2) \mid 2^k$ dan $\text{ord}_p(2) \nmid 2^{k-1}$. Maka $\text{ord}_p(2) = 2^k$ dan dari **Lemma 1.3**, kita punya $2^k \mid p-1 \implies 2^k \leq p-1 \implies p > 2^k$. Maka terbukti bahwa $\sigma(n)$ memiliki faktor prima yang lebih besar dari 2^k. ■

> **Remark.** Penentuan $\nu_p(n!)$ untuk suatu bilangan prima p dan bilangan asli n dapat ditentukan dengan
>
> $$\nu_p(n!) = \sum_{i\geq 1} \left\lfloor \frac{n}{p^i} \right\rfloor \quad \text{atau} \quad \nu_p(n!) = \frac{n - s_p(n)}{p-1}$$
>
> di mana $s_p(n)$ menyatakan jumlah digit-digit dari n dalam basis p.

Pustaka

[1] Chen, Evan. (2015). *Orders Modulo A Prime*. https://web.evanchen.cc/handouts/ORPR/ORPR.pdf, diakses tanggal 2 Mei 2022.

[2] Khurmi, Aditya. (2020). *Modern Olympiad Number Theory*. https://artofproblemsolving.com/community/c6h2344755, diakses tanggal 2 Mei 2022.

[3] Raji, Wissam. (2021). *The Existence of Primitive Roots*. https://math.libretexts.org/Bookshelves/Combinatorics_and_Discrete_Mathematics/Elementary_Number_Theory_(Raji)/05%3A_Primitive_Roots_and_Quadratic_Residues/5.03%3A_The_Existence_of_Primitive_Roots, diakses tanggal 3 Mei 2022.

[4] Stevens, Justin. (Tanpa Tahun). *Olympiad Number Theory Through Challenging Problems*, [pdf]. https://s3.amazonaws.com/aops-cdn.artofproblemsolving.com/resources/articles/olympiad-number-theory.pdf, diakses tanggal 3 Mei 2022.