Zad. 7

a) $xz \equiv yz \pmod{mz}$

$(\Leftarrow)$ $\Updownarrow$

$mz \mid xz - yz \Leftrightarrow mz \mid (x-y)z \Leftrightarrow m \mid x-y \Leftrightarrow x \equiv y \mod m$

b) ~~$xz \equiv yz \pmod{m}$~~

$(\Leftarrow)$

$xz \equiv yz \ (m) \Leftrightarrow m \mid xz - yz \Leftrightarrow m \mid (x-y)z \Leftrightarrow \frac{m}{\gcd(z,m)} \mid (x-y)\frac{z}{\gcd(z,m)} \Leftrightarrow \frac{m}{\gcd(z,m)} \mid x-y \Leftrightarrow x \equiv y \ (\mod \frac{m}{\gcd(z,m)})$

WZGLĘDNIE PIERWSZE

c)

$k \in \mathbb{Z}$

$x \equiv y \pmod{mz} \Rightarrow mz \mid x-y \Rightarrow mz \cdot k = x-y \Rightarrow m \cdot (z \cdot k) = x-y \Rightarrow m \mid x-y \Leftrightarrow x \equiv y \pmod{m}$

Zad. 8

a) zał $2^n - 1$ pierwsza

Jeżeli n nie jest pierwsza to $n = xy$, $x, y \in \mathbb{Z}$. Więc $2^n - 1 = 2^{xy} - 1 = (2^x - 1)\left(\sum_{i=0}^{y-1} 2^{x \cdot i}\right)$ więc $2^n - 1$ też nie pierwsza

za z kontrapozycji n pierwsza.

b) Zał: $a^n - 1$ pierwsza:

$a^n - 1 = (a-1)\left(\sum_{i=0}^{n-1} a^i 1^{n-i-1}\right)$ aby liczba po prawej równa była pierwsza to musi być iloczyn 1 i siebie samej $a-1 \neq a^n - 1$ dla dalszego więc $a-1 = 1 \Rightarrow a = 2$, $\left(\sum_{i=0}^{n-1} 2^i = 2^n - 1\right)$ ✓.

c) zał: $2^n + 1$ pierwsza:

Zał, nie wprost, że $n = 2^a k$ więc $2^n + 1 = (2^{2^a})^k + 1 = (2^{2^a} + 1)\left(\sum_{i=0}^{k-1} (2^{2^a})^{k-i-1}\right)$

$\neq 1$, $\neq 2^n + 1$

zatem 2^{n+1} złożona ↯

Zad. 12

$*$
$$\begin{cases} x \equiv 11 \mod 27 \\ x \equiv 12 \mod 64 \\ x \equiv 13 \mod 25 \end{cases}$$

$$x = 11 l \cdot 64 \cdot 25 + 12 \overbrace{m \cdot 27 \cdot 25}^{\substack{0 \bmod 27 \\ 0 \bmod 25}} + 13 \cdot n \cdot 27 \cdot 64$$

. Dobieramy pozostałe l, m, n by spełniały $*$. $l = (25 \cdot 64)^{-1} \pmod{27}$ itd.

$64 \cdot 25 \equiv 7 \mod 27$

Używamy rozszerzonego algorytmu euklidesa:

$64 \cdot 25 \cdot l \equiv 1 \mod 27$
$7 \cdot l = 1$
$l = 4$

$27 \cdot 25 \cdot m \equiv 1 \mod 64$
$35 m \equiv 1 \mod 64$
$m = 11$

$64 \cdot 27 \cdot n \equiv 1 \mod 25$
$14 \cdot 2 \cdot n \equiv 1$
$3 \cdot n \equiv 1$
$n = 17$

$$x = 11 \cdot 4 \cdot 64 \cdot 25 + 12 \cdot 11 \cdot 27 \cdot 25 + 13 \cdot 17 \cdot 27 \cdot 64 = 541\,388$$

$$x = 541\,388 \mod 27 \cdot 25 \cdot 64 = 22\,988$$

Zad. 13

5	7	9	11	179
4	3	6	10	178

argument

komdersay

$\mathrm{lcm}(4,3,6,10,178) = 5340$

$2^{m_1} \equiv 1 \bmod k_1$

$2^{m_2} \equiv 1 \bmod k_2$

gcd

$2^{\mathrm{lcm}(m_1,m_2)} = 2^{p_1 \cdot m_1} = 2^{p_2 \cdot m_2} \stackrel{\text{mod } k_1}{=} q_1 k_1 + 1 = q_2 \cdot k_2 + 1 \equiv 1 \bmod k_1 k_2$

Zad. 14

teza: $\sum_{k=1}^{n} d(k) = n \ln n + O(n)$

Liczb podzielnych przez k jest $\lfloor \frac{n}{k} \rfloor$

$O(n)$

$\sum_{k=1}^{n} d(k) = \lfloor \frac{n}{1} \rfloor + \lfloor \frac{n}{2} \rfloor + \ldots + \lfloor \frac{n}{n} \rfloor \leq \frac{n}{1} + \frac{n}{2} + \ldots + \frac{n}{n} = n\left(\frac{1}{1} + \frac{1}{2} + \ldots + \frac{1}{n}\right) \leq n \ln(n+1) = n \ln n + O(n)$

$\blacksquare$

Zad. 9 • $2 \mid ((2-1)!+1)$ V

• $p \geq 3$

• Rozważ wielomian: • $g(x) = (x-1) \cdot \ldots \cdot (x-(p-1))$, stopień: p-1, wyraz o najw. potędze x^{p-1}, WYRAZ WOLNY: $(p-1)!$

$1, 2, \ldots, p-1 \leftarrow$ pierwiastki

• $h(x) = x^{p-1} - 1$ z MTF $h(x) = 0$ dla $p \nmid x$ w tym $x \in \{1, \ldots, p-1\}$

$f(x) = g(x) - h(x)$ Zatem $g(x)$ i $h(x)$ mają te same p-1 pierwiastków: $1, 2, \ldots, p-1$

$f(x)$ stopnia $p-2$ bo wyraz x^{p-1} się usuwa, ale ma p-1 pierwiastków: $1, 2, \ldots, p-1$

z ~~tw. Lagrange'a~~ nie może mieć więcej niż $p-2$ (stopień) pierwiastków, zatem $f(x) \equiv 0$

zasadniczego tw. Algebry

$g(x) - h(x) \equiv 0 \implies p-1! + 1 \equiv 0 \mod p$

WYRAZ wolny $g(x)$ — WYRAZ wolny $h(x)$

Zad. 10

$x^2 \equiv 1 \mod p^\alpha$

$(x+1)(x-1) \equiv 0 \mod p^\alpha$

1° $p > 2$ wtedy $(x+1) \not\equiv (x-1) \mod p^\alpha$

więc: $p^\alpha \mid x-1$ lub $p^\alpha \mid x+1$

$x = 1$

$x = p^\alpha - 1$

2° $p = 2$

$\alpha = 1$ $(x+1)(x-1) \equiv 0 \mod 2$ $x = 1$ 1

$\alpha = 2$ $(x+1)(x-1) \equiv 0 \mod 4$ $x = 1, x = 3$ 2

$\alpha \geq 3$

$2^{\alpha-1} \mid (x-1) \implies 2 \mid (x+1)$

$x = 2^\alpha \pm 1$ V $x = 2^{\alpha-1} \pm 1$ 4 rozw.