Diskrétní matematika – cvičení 5. týden

Lukáš Vokřínek

Masarykova univerzita
Fakulta informatiky

jaro 2020

Příklad

Pětice modulů 3; 5; 7; 11; 13 umožňuje jednoznačně reprezentovat čísla menší než jejich součin (tedy menší než 15015) a efektivně provádět (v případě potřeby distribuovaně) běžné aritmetické operace. Určete reprezentaci čísel 1234 a 5678 v této modulární soustavě a pomocí této reprezentace vypočtěte jejich součet a součin.

Příklad

Pětice modulů 3; 5; 7; 11; 13 umožňuje jednoznačně reprezentovat čísla menší než jejich součin (tedy menší než 15015) a efektivně provádět (v případě potřeby distribuovaně) běžné aritmetické operace. Určete reprezentaci čísel 1234 a 5678 v této modulární soustavě a pomocí této reprezentace vypočtěte jejich součet a součin.

Řešení

$$\begin{aligned}
1234 &\equiv 1 \pmod{3} & \qquad 5678 &\equiv 2 \pmod{3}\\
1234 &\equiv 4 \pmod{5} & \qquad 5678 &\equiv 3 \pmod{5}\\
1234 &\equiv 2 \pmod{7} & \qquad 5678 &\equiv 1 \pmod{7}\\
1234 &\equiv 2 \pmod{11} & \qquad 5678 &\equiv 2 \pmod{11}\\
1234 &\equiv 12 \pmod{13} & \qquad 5678 &\equiv 10 \pmod{13}
\end{aligned}$$

Řešení

$$1234 \equiv 1 \pmod{3} \qquad 5678 \equiv 2 \pmod{3}$$
$$1234 \equiv 4 \pmod{5} \qquad 5678 \equiv 3 \pmod{5}$$
$$1234 \equiv 2 \pmod{7} \qquad 5678 \equiv 1 \pmod{7}$$
$$1234 \equiv 2 \pmod{11} \qquad 5678 \equiv 2 \pmod{11}$$
$$1234 \equiv 12 \pmod{13} \qquad 5678 \equiv 10 \pmod{13}$$

Řešení

$$
\begin{aligned}
1234 &\equiv 1 \pmod 3 & \qquad 5678 &\equiv 2 \pmod 3\\
1234 &\equiv 4 \pmod 5 & \qquad 5678 &\equiv 3 \pmod 5\\
1234 &\equiv 2 \pmod 7 & \qquad 5678 &\equiv 1 \pmod 7\\
1234 &\equiv 2 \pmod{11} & \qquad 5678 &\equiv 2 \pmod{11}\\
1234 &\equiv 12 \pmod{13} & \qquad 5678 &\equiv 10 \pmod{13}
\end{aligned}
$$

Reprezentujeme tedy číslo 1234 pomocí pětice zbytků $(1, 4, 2, 2, 12)$ a číslo 5678 pomocí pětice zbytků $(2, 3, 1, 2, 10)$. Součet a součin jsou pak reprezentovány

$$
\begin{aligned}
1234 + 5678 &\sim (3, 7, 3, 4, 22) \equiv (0, 2, 3, 4, 9)\\
1234 \cdot 5678 &\sim (2, 12, 2, 4, 120) \equiv (2, 2, 2, 4, 3)
\end{aligned}
$$

Řešení

$$1234 + 5678 \sim (0, 2, 3, 4, 9)$$

Převeďme nyní tyto reprezentace zpět na čísla, řešme tedy v prvním případě soustavu kongruencí

$$\begin{aligned} x &\equiv 0 \pmod{3} \\ x &\equiv 2 \pmod{5} \\ x &\equiv 3 \pmod{7} \\ x &\equiv 4 \pmod{11} \\ x &\equiv 9 \pmod{13} \end{aligned}$$

Řešení

$$1234 + 5678 \sim (0, 2, 3, 4, 9)$$

Převeďme nyní tyto reprezentace zpět na čísla, řešme tedy v prvním případě soustavu kongruencí

$$\begin{aligned}
x &\equiv 0 \pmod 3\\
x &\equiv 2 \pmod 5\\
x &\equiv 3 \pmod 7\\
x &\equiv 4 \pmod{11}\\
x &\equiv 9 \pmod{13}
\end{aligned}$$

Z první kongruence máme $x = 3t$, dosazením do druhé dostaneme kongruenci $3t \equiv 2 \pmod 5$, tedy $t \equiv 4 \pmod 5$, tj. $t = 5s + 4$ a $x = 15s + 12$.

Řešení

$$1234 + 5678 \sim (0, 2, 3, 4, 9)$$

Převeďme nyní tyto reprezentace zpět na čísla, řešme tedy v prvním případě soustavu kongruencí

$$\begin{aligned} x &\equiv 0 \pmod 3 \\ x &\equiv 2 \pmod 5 \\ x &\equiv 3 \pmod 7 \\ x &\equiv 4 \pmod{11} \\ x &\equiv 9 \pmod{13} \end{aligned}$$

Z první kongruence máme $x = 3t$, dosazením do druhé dostaneme kongruenci $3t \equiv 2 \pmod 5$, tedy $t \equiv 4 \pmod 5$, tj. $t = 5s + 4$ a $x = 15s + 12$. Dosadíme do třetí kongruence: $15s \equiv -9 \pmod 7$, tedy $s \equiv 5 \pmod 7$, tj. $s = 7r + 5 \Rightarrow x = 105r + 87$.

Řešení

$$
\begin{aligned}
x &\equiv 0 \pmod{3}\\
x &\equiv 2 \pmod{5}\\
x &\equiv 3 \pmod{7}\\
x &\equiv 4 \pmod{11}\\
x &\equiv 9 \pmod{13}
\end{aligned}
$$

Dosadíme $x = 105r + 87$ do čtvrté kongruence a dostaneme $105r \equiv -83 \pmod{11}$, tedy $6r \equiv 5 \pmod{11} \Rightarrow r \equiv 10 \pmod{11}$, tj. $r = 11q + 10$ a $x = 1155q + 1137$.

Řešení

$$
\begin{aligned}
x &\equiv 0 \pmod{3} \\
x &\equiv 2 \pmod{5} \\
x &\equiv 3 \pmod{7} \\
x &\equiv 4 \pmod{11} \\
x &\equiv 9 \pmod{13}
\end{aligned}
$$

Dosadíme $x = 105r + 87$ do čtvrté kongruence a dostaneme $105r \equiv -83 \pmod{11}$, tedy $6r \equiv 5 \pmod{11} \Rightarrow r \equiv 10 \pmod{11}$, tj. $r = 11q + 10$ a $x = 1155q + 1137$. Dosadíme do poslední kongruence a dostaneme $1155q \equiv -1128 \pmod{13}$, tedy $11q \equiv 3 \pmod{13}$:

Řešení

$$\begin{aligned} 13q &\equiv 0 \\ 11q &\equiv 3 \\ 2q &\equiv 10 \\ 1q &\equiv 5 \pmod{13} \\ 0q &\equiv 0 \end{aligned}$$

Máme tak $q = 13p + 5$ a dosazením $x = 15015p + 6912$, tj. $x \equiv 6912 \pmod{15015}$.

Řešení

$$\begin{aligned}
13q &\equiv 0\\
11q &\equiv 3\\
2q &\equiv 10\\
1q &\equiv 5 \pmod{13}\\
0q &\equiv 0
\end{aligned}$$

Máme tak $q = 13p + 5$ a dosazením $x = 15015p + 6912$, tj. $x \equiv 6912 \pmod{15015}$. Protože je součet menší než 15015, musí nutně být roven 6912.

Řešení

Podobně v případě součinu $1234 \cdot 5678 \sim (2, 2, 2, 4, 3)$:

$$
\begin{aligned}
x &\equiv 2 \pmod 3\\
x &\equiv 2 \pmod 5\\
x &\equiv 2 \pmod 7\\
x &\equiv 4 \pmod{11}\\
x &\equiv 3 \pmod{13}
\end{aligned}
$$

dostáváme z prvních tří kongruencí $x = 105r + 2$ (protože je pravá strana stejná), dosadíme do čtvrté: $105r \equiv 6r \equiv 2 \pmod{11}$, tedy $r \equiv 4 \pmod{11}$, tj. $r = 11q + 4$ a $x = 1155q + 422$.

Řešení

Podobně v případě součinu $1234 \cdot 5678 \sim (2, 2, 2, 4, 3)$:

$$\begin{aligned}
x &\equiv 2 \pmod{3} \\
x &\equiv 2 \pmod{5} \\
x &\equiv 2 \pmod{7} \\
x &\equiv 4 \pmod{11} \\
x &\equiv 3 \pmod{13}
\end{aligned}$$

dostáváme z prvních tří kongruencí $x = 105r + 2$ (protože je pravá strana stejná), dosadíme do čtvrté: $105r \equiv 6r \equiv 2 \pmod{11}$, tedy $r \equiv 4 \pmod{11}$, tj. $r = 11q + 4$ a $x = 1155q + 422$. Dosadíme do poslední kongruence a dostaneme $1155q \equiv -419 \pmod{13}$, tedy $11q \equiv 10 \pmod{13}$:

Řešení

$$\begin{aligned} 13q &\equiv 0 \\ 11q &\equiv 10 \\ 2q &\equiv 3 \\ 1q &\equiv 8 \pmod{13} \\ 0q &\equiv 0 \end{aligned}$$

Máme tak $q = 13p + 8$ a dosazením $x = 15015p + 9662$, tj. $x \equiv 9662 \pmod{15015}$.

Řešení

$$
\begin{aligned}
13q &\equiv 0 \\
11q &\equiv 10 \\
2q &\equiv 3 \\
1q &\equiv 8 \pmod{13} \\
0q &\equiv 0
\end{aligned}
$$

Máme tak $q = 13p + 8$ a dosazením $x = 15015p + 9662$, tj. $x \equiv 9662 \pmod{15015}$. Kdyby byl součin menší než 15015, musel by nutně být roven 9662; ve skutečnosti ale došlo k “přetečení”.

Příklad

Ukažte, že jsou čísla $2^n - 1$; 2^n; $2^n + 1$ po dvou nesoudělná a určete, kolik bitů mohou mít jimi určená čísla. Spočtěte reprezentaci čísla 118 v této soustavě s $n = 3$. Zapřemýšlejte o efeketivní realizaci této modulární aritmetiky.

Příklad

Ukažte, že jsou čísla $2^n - 1$; 2^n; $2^n + 1$ po dvou nesoudělná a určete, kolik bitů mohou mít jimi určená čísla. Spočtěte reprezentaci čísla 118 v této soustavě s $n = 3$. Zapřemýšlejte o efeketivní realizaci této modulární aritmetiky.

Řešení

Ukážeme nesoudělnost $2^n - 1$ a $2^n + 1$, nesoudělnost dvou po sobě jdoucích čísel je ještě snazší. Počítejme:

$$(2^n - 1, 2^n + 1) = (2^n - 1, 2) = (-1, 2) = (1, 2) = 1$$

(od $2^n + 1$ lze odečíst $2^n - 1$ a zbude 2, v dalším kroku lze od $2^n - 1$ odečíst 2^n, protože se jedná o násobek 2).

Příklad

Ukažte, že jsou čísla $2^n - 1$; 2^n; $2^n + 1$ po dvou nesoudělná a určete, kolik bitů mohou mít jimi určená čísla. Spočtěte reprezentaci čísla 118 v této soustavě s $n = 3$. Zapřemýšlejte o efeketivní realizaci této modulární aritmetiky.

Řešení

Podle CRT pak trojice zbytků jednoznačně reprezentuje čísla modulo

$$[2^n - 1, 2^n, 2^n + 1] = (2^n - 1) \cdot 2^n \cdot (2^n + 1) = 2^{3n} - 2^n,$$

tedy téměř všechna čísla čítající $3n$ bitů.

Řešení

Pišme nyní vše ve dvojkové soustavě: máme tak spočítat zbytek po dělení čísla sto osmnáct, tedy $1\,110\,110$, modulo sedm, osm, devět, tedy 111, $1\,000$, $1\,001$.

Řešení

Pišme nyní vše ve dvojkové soustavě: máme tak spočítat zbytek po dělení čísla sto osmnáct, tedy $1\,110\,110$, modulo sedm, osm, devět, tedy 111, $1\,000$, $1\,001$. Přesněji pišme dané číslo po trojicích cifer jako

$$1\,110\,110 = 1 \cdot 1000^2 + 110 \cdot 1000 + 110$$

Řešení

Pišme nyní vše ve dvojkové soustavě: máme tak spočítat zbytek po dělení čísla sto osmnáct, tedy $1\,110\,110$, modulo sedm, osm, devět, tedy 111, $1\,000$, $1\,001$. Přesněji pišme dané číslo po trojicích cifer jako

$$1\,110\,110 = 1 \cdot 1000^2 + 110 \cdot 1000 + 110$$

Pak modulo $1\,000$ je jistě

$$1\,110\,110 \equiv 110 \pmod{1000}.$$

Řešení

Pišme nyní vše ve dvojkové soustavě: máme tak spočítat zbytek po dělení čísla sto osmnáct, tedy $1\,110\,110$, modulo sedm, osm, devět, tedy 111, $1\,000$, $1\,001$. Přesněji pišme dané číslo po trojicích cifer jako

$$1\,110\,110 = 1 \cdot 1000^2 + 110 \cdot 1000 + 110$$

Pak modulo $1\,000$ je jistě

$$1\,110\,110 \equiv 110 \pmod{1000}.$$

Protože je $1\,000 \equiv 1 \pmod{111}$, dostáváme

$$1\,110\,110 \equiv 1 + 110 + 110 \equiv 1\,101 \equiv 110 \pmod{111}.$$

Řešení

Pišme nyní vše ve dvojkové soustavě: máme tak spočítat zbytek po dělení čísla sto osmnáct, tedy 1 110 110, modulo sedm, osm, devět, tedy 111, 1 000, 1 001. Přesněji pišme dané číslo po trojicích cifer jako

$$1\,110\,110 = 1 \cdot 1000^2 + 110 \cdot 1000 + 110$$

Pak modulo 1 000 je jistě

$$1\,110\,110 \equiv 110 \pmod{1000}.$$

Protože je $1\,000 \equiv 1 \pmod{111}$, dostáváme

$$1\,110\,110 \equiv 1 + 110 + 110 \equiv 1\,101 \equiv 110 \pmod{111}.$$

Protože je $1\,000 \equiv -1 \pmod{1\,001}$, dostáváme

$$1\,110\,110 \equiv 1 - 110 + 110 \equiv 1 \pmod{1001}.$$

Příklad

Šifrou RSA s veřejným klíčem $e = 7$, $n = p \cdot q = 33$ byly poslány tři zprávy 29, 7, 21. Prolomte šifru a zprávy dešifrujte.

Řešení

Zatímco $n = p \cdot q$ je veřejným klíčem, jednotlivá prvočísla p, q jsou soukromým klíčem.

Příklad

Šifrou RSA s veřejným klíčem $e = 7$, $n = p \cdot q = 33$ byly poslány tři zprávy 29, 7, 21. Prolomte šifru a zprávy dešifrujte.

Řešení

Zatímco $n = p \cdot q$ je veřejným klíčem, jednotlivá prvočísla p, q jsou soukromým klíčem. Rozklad se využije k výpočtu Eulerovy funkce

$$\varphi(n) = (p-1)(q-1),$$

pomocí níž je určen soukromý klíč d:

$$e \cdot d \equiv 1 \pmod{\varphi(n)}.$$

Příklad

Šifrou RSA s veřejným klíčem $e = 7$, $n = p \cdot q = 33$ byly poslány tři zprávy 29, 7, 21. Prolomte šifru a zprávy dešifrujte.

Řešení

Zatímco $n = p \cdot q$ je veřejným klíčem, jednotlivá prvočísla p, q jsou soukromým klíčem. Rozklad se využije k výpočtu Eulerovy funkce

$$\varphi(n) = (p-1)(q-1),$$

pomocí níž je určen soukromý klíč d:

$$e \cdot d \equiv 1 \pmod{\varphi(n)}.$$

Šifrování čísla $m \pmod{n}$ je dáno umocňováním na e, tj. $c \equiv m^e \pmod{n}$. Dešifrování je pak dáno umocňováním na d, tj. $m \equiv c^d \pmod{n}$, protože díky Eulerově větě platí:

$$c^d \equiv (m^e)^d \equiv m^{e \cdot d} \equiv m^1 \equiv m \pmod{n}.$$

Příklad

Šifrou RSA s veřejným klíčem $e = 7$, $n = p \cdot q = 33$ byly poslány tři zprávy 29, 7, 21. Prolomte šifru a zprávy dešifrujte.

Řešení

Prolomení šifry spočívá ve faktorizaci čísla 33, tj. v nalezení prvočísel p, q. V našem případě je to jednoduché: $p = 3$, $q = 11$, zejména tak

$$\varphi(p \cdot q) = (p-1)(q-1) = 2 \cdot 10 = 20.$$

Příklad

Šifrou RSA s veřejným klíčem $e = 7$, $n = p \cdot q = 33$ byly poslány tři zprávy 29, 7, 21. Prolomte šifru a zprávy dešifrujte.

Řešení

Prolomení šifry spočívá ve faktorizaci čísla 33, tj. v nalezení prvočísel p, q. V našem případě je to jednoduché: $p = 3$, $q = 11$, zejména tak

$$\varphi(p \cdot q) = (p-1)(q-1) = 2 \cdot 10 = 20.$$

Nyní můžeme spočítat inverzi d k $e \equiv 7 \pmod{\varphi(n)}$, totiž

$$\begin{aligned} 20d &\equiv 0 \\ 7d &\equiv 1 \\ 6d &\equiv -2 \\ 1d &\equiv 3 \pmod{20} \end{aligned}$$

Příklad

Šifrou RSA s veřejným klíčem $e = 7$, $n = p \cdot q = 33$ byly poslány tři zprávy 29, 7, 21. Prolomte šifru a zprávy dešifrujte.

Řešení

Dešifrování se tedy provádí umocňováním na třetí modulo n, pro jednotlivé zprávy vychází

$$
\begin{aligned}
m_1 &\equiv 29^3 \equiv 2 \pmod{33} \\
m_2 &\equiv 7^3 \equiv 13 \pmod{33} \\
m_3 &\equiv 21^3 \equiv 21 \pmod{33}
\end{aligned}
$$

Příklad

Šifrou RSA s veřejným klíčem $e = 7$, $n = p \cdot q = 33$ byly poslány tři zprávy 29, 7, 21. Prolomte šifru a zprávy dešifrujte.

Řešení

Dešifrování se tedy provádí umocňováním na třetí modulo n, pro jednotlivé zprávy vychází

$$\begin{aligned} m_1 &\equiv 29^3 \equiv 2 \pmod{33} \\ m_2 &\equiv 7^3 \equiv 13 \pmod{33} \\ m_3 &\equiv 21^3 \equiv 21 \pmod{33} \end{aligned}$$

(u poslední zprávy je nicméně jak původní tak zašifrovaná zpráva soudělná s modulem, což je velmi nevhodné, protože tak lze pomocí největšího společného dělitele rozložit modul).

Příklad

Demonstrujte RSA protokol se zvolenými prvočísly 23 a 29 s vhodnou volbou veřejného klíče e. Zašifrujte a odšifrujte několik zpráv m pro ne moc velká m.

Řešení

Máme $n = p \cdot q = 667$. Budeme volit $e = 487$ a $m \equiv 25 \pmod{667}$. Zašifrovaná zpráva pak je $c \equiv 25^{487} \pmod{667}$.

Příklad

Demonstrujte RSA protokol se zvolenými prvočísly 23 a 29 s vhodnou volbou veřejného klíče e. Zašifrujte a odšifrujte několik zpráv m pro ne moc velká m.

Řešení

Máme $n = p \cdot q = 667$. Budeme volit $e = 487$ a $m \equiv 25 \pmod{667}$.
Zašifrovaná zpráva pak je $c \equiv 25^{487} \pmod{667}$.
Ukážeme, jak lze mocninu (snadněji?) počítat zvlášť modulo 23 a 29 (to samozřejmě bez znalosti faktorizace nelze, jde jen o zjednodušení pro účely příkladu):

Příklad

Demonstrujte RSA protokol se zvolenými prvočísly 23 a 29 s vhodnou volbou veřejného klíče e. Zašifrujte a odšifrujte několik zpráv m pro ne moc velká m.

Řešení

Máme $n = p \cdot q = 667$. Budeme volit $e = 487$ a $m \equiv 25 \pmod{667}$.
Zašifrovaná zpráva pak je $c \equiv 25^{487} \pmod{667}$.
Ukážeme, jak lze mocninu (snadněji?) počítat zvlášť modulo 23 a 29 (to samozřejmě bez znalosti faktorizace nelze, jde jen o zjednodušení pro účely příkladu):

$$c \equiv 25^{487} \equiv 2^3 \equiv 8 \pmod{23}$$
$$c \equiv 25^{487} \equiv (-4)^{11} \equiv -5 \pmod{29}$$

(exponenty lze redukovat modulo $\varphi(23)$, resp. $\varphi(29)$).

Příklad

Demonstrujte RSA protokol se zvolenými prvočísly 23 a 29 s vhodnou volbou veřejného klíče e. Zašifrujte a odšifrujte několik zpráv m pro ne moc velká m.

Řešení

Nyní dáme tyto dva mezivýsledky, $c \equiv 8 \pmod{23}$, $c \equiv -5 \pmod{29}$, dohromady modulo 667:

Příklad

Demonstrujte RSA protokol se zvolenými prvočísly 23 a 29 s vhodnou volbou veřejného klíče e. Zašifrujte a odšifrujte několik zpráv m pro ne moc velká m.

Řešení

Nyní dáme tyto dva mezivýsledky, $c \equiv 8 \pmod{23}$, $c \equiv -5 \pmod{29}$, dohromady modulo 667:

$$\begin{aligned}
29c &\equiv 8 \cdot 29 \\
23c &\equiv \qquad\qquad -5 \cdot 23 \\
6c &\equiv 8 \cdot 29 + 5 \cdot 23 \\
5c &\equiv -24 \cdot 29 - 20 \cdot 23 \equiv -1 \cdot 29 + 9 \cdot 23 \\
c &\equiv 9 \cdot 29 - 4 \cdot 23 \equiv 169
\end{aligned}$$

Řešení

Podobně budeme i dešifrovat, prvně potřebujeme k veřejnému klíči $e = 487$ spočítat soukromý klíč d, tj. inverzi modulo $\varphi(23 \cdot 29) = 22 \cdot 28 = 616$:

$$\begin{aligned}
616d &\equiv 0 \\
487d &\equiv 1 \\
129d &\equiv -1 \\
100d &\equiv 4 \\
29d &\equiv -5 \\
13d &\equiv 19 \\
3d &\equiv -43 \\
1d &\equiv 191 \pmod{616}
\end{aligned}$$

Příklad

Demonstrujte RSA protokol se zvolenými prvočísly 23 a 29 s vhodnou volbou veřejného klíče e. Zašifrujte a odšifrujte několik zpráv m pro ne moc velká m.

Řešení

Dešifrovaná zpráva je $m \equiv 169^{191} \pmod{667}$:

Příklad

Demonstrujte RSA protokol se zvolenými prvočísly 23 a 29 s vhodnou volbou veřejného klíče e. Zašifrujte a odšifrujte několik zpráv m pro ne moc velká m.

Řešení

Dešifrovaná zpráva je $m \equiv 169^{191} \pmod{667}$:

$$m \equiv 169^{191} \equiv 8^{-7} \equiv (8^{-1})^7 \equiv 3^7 \equiv 2 \pmod{23}$$
$$m \equiv 169^{191} \equiv (-5)^{-5} \equiv ((-5)^{-1})^5 \equiv (-6)^5 \equiv -4 \pmod{29}$$

(mocniny se záporným exponentem lze počítat pomocí inverze).

Příklad

Demonstrujte RSA protokol se zvolenými prvočísly 23 a 29 s vhodnou volbou veřejného klíče e. Zašifrujte a odšifrujte několik zpráv m pro ne moc velká m.

Řešení

Nyní dáme tyto dva mezivýsledky, $m \equiv 2 \pmod{23}$, $m \equiv -4 \pmod{29}$, dohromady modulo 667:

Příklad

Demonstrujte RSA protokol se zvolenými prvočísly 23 a 29 s vhodnou volbou veřejného klíče e. Zašifrujte a odšifrujte několik zpráv m pro ne moc velká m.

Řešení

Nyní dáme tyto dva mezivýsledky, $m \equiv 2 \pmod{23}$, $m \equiv -4 \pmod{29}$, dohromady modulo 667:

$$\begin{aligned}
29m &\equiv 2 \cdot 29 \\
23m &\equiv \qquad\qquad -4 \cdot 23 \\
6m &\equiv 2 \cdot 29 + 4 \cdot 23 \\
5m &\equiv -6 \cdot 29 - 16 \cdot 23 \\
m &\equiv 8 \cdot 29 + 20 \cdot 23 \equiv 692 \equiv 25
\end{aligned}$$