Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

POLINOMSKI ALGORITMI ZA TESTIRANJE PRAŠTEVILSKOSTI

magistrska naloga

Miha Vuk

mentor: prof. dr. Borut Robič

Ljubljana, 2006

Predstavili bomo:

1. kaj praštevila so
2. splošno o algoritmih za njihovo razpoznavanje
3. algoritem Agrawal-Kayal-Saxsena
4. ekperimentalna in teoretična primerjava

Praštevila

Praštevila so števila, ki niso deljiva s števili manjšimi od njih. Zato jih tudi ne moremo zapisati kot produkt.

Primer:

$2 = 2$	praštevilo
$3 = 3$	praštevilo
$4 = 2 \cdot 2$	sestavljeno število
$5 = 5$	praštevilo
$6 = 2 \cdot 3$	sestavljeno število

Prime numbers are what is left when you have taken all the patterns away. I think prime numbers are like life. They are very logical but you could never work out the rules, even if you spent all your time thinking about them.

(iz knjige Marka Haddona:
The Curious Incident of the
Dog in Night-time)

Vrste algoritmov

1. splošni in posebni (za posebna števila)
2. deterministični in verjetnostni
3. dokazano pravilni in domnevno pravilni

Gostota praštevil

Praštevilski izrek

$$\pi(n) \sim \frac{n}{\ln n},$$

kjer je $\pi(n)$ število vseh praštevil manjših od n.

Torej je vseh praštevil neskončno.

Lastnosti praštevil

Fermatov mali izrek

Definirajmo

$$\phi(n) = |\{a \mid a < n,\ a|n\}|,$$

kar da za praštevila p

$$\phi(p) = p - 1.$$

Fermat je pokazal, da za praštevila p in $1 \leq a < p$ velja

$$a^{p-1} \equiv 1 \pmod{p},$$

podobno pa tudi za vsak a, ki je tuj z n, velja

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

PRIMES **je v razredu NP in n-1 testi**

Lucasov test

Naj bo $n > 1$. Potem je n praštevilo natanko takrat, ko obstaja a, $1 < a < n$, da velja

- $a^{n-1} \equiv 1 \pmod{n}$ in
- $a^{(n-1)/q} \not\equiv 1 \pmod{n}$, za vsak praštevilski delitelj q števila $n - 1$.

Test je uporaben, če znamo faktorizirati $n - 1$.

Podobno obstajajo testi, ki temeljijo na faktorizaciji drugih polinomov s spremenljivko n (predvsem $n + 1$ in $n^m - 1$).

Mersennova (pra)števila

Za števila oblike $n = 2^s - 1$ poznamo izjemno učinkovit $(n+1)$ test. Z njim je dokazano trenutno največje znano praštevilo $2^{32582657} - 1$.

LUCAS-LEHMERJEV TEST

VHOD: Mersennovo število $n = 2^s - 1$ za $s \geq 3$.

1. S poskusnim deljenjem preveri, da s nima deliteljev manjših od $\lfloor\sqrt{s}\rfloor$. Če jih ima, zaključi("sestavljeno število").
2. u := 4
3. **for** $k := 1, \ldots, s-2$ **do**
   $u := (u^2 - 2) \pmod{n}$
4. **if** $(u = 0)$ **then**
   zaključi("praštevilo")
   else
   zaključi("sestavljeno število")

Verjetnostni in deterministični algoritmi

FERMATOV TEST

VHOD: liho število $n \geq 3$..
IZHOD: odgovor "sestavljeno število" ali "možno praštevilo".

1. Izberi naključno število a, $2 \leq a \leq n-2$.
2. **if** $(a^{n-1} \not\equiv 1 \pmod{n})$ **then** zaključi("sestavljeno število")
3. Zaključi("možno praštevilo").

OSNOVNI RABINOV ALGORITEM

VHOD: liho število $n \geq 3$.

1. Izberi naključno število a, $1 \leq a \leq n-1$.
2. **if** $(a^{n-1} \not\equiv 1 \pmod{n})$ **then** zaključi("sestavljeno število")
3. **if** (obstaja i, tako da $2^i | (n-1)$ in $1 < gcd(a^{(n-1)/2^i} - 1, n) < n$) **then** zaključi("sestavljeno število")
4. Zaključi("možno praštevilo").

Najboljši algoritmi pred letom 2002

- Rabin-Millerjev verjetnostni algoritem, kadar ne potrebujemo dokaza praštevilskosti
- algoritem APR-CL (deterministično skoraj polinomski, faktorizacija $n^m - 1$)
- algoritem ECCP (s polinomskim pričakovanim časom izvajanja), (pomanjkljiv dokaz, da deluje za vsa števila)

Algoritem Agrawal-Kayal-Saxsena

- prvi pravi polinomski deterministič̆en algoritem
- prvič objavljen leta 2002
- izjemen odziv javnosti
- še zelo počasen (dokazana zahtevnost $\mathcal{O}^{\sim}(\log^{12} n)$, a v praksi blizu $\mathcal{O}^{\sim}(\log^{6} n)$)

Algoritem Agrawal-Kayal-Saxsena

Osnovna ideja

Naj bo $a \in \mathbb{Z}$, $n \in \mathbb{N}$, $n \geq 2$ in $gcd(a, n) = 1$. Potem je n praštevilo natanko takrat, ko velja

$$(X + a)^n \equiv X^n + a \pmod{n}.$$

Preverjenja te enakosti je izjemno računsko zahtevno, zato se omejimo na njen približek

$$(X + a)^n \equiv X^n + a \pmod{X^r - 1, n}. \tag{1}$$

za nek primerno majhen r.

Algoritem AKS preverja enakost (1) za majhno množico a-jev.

Algoritem Agrawal-Kayal-Saxsena

ALGORITEM AKS (`AKS-v3`)

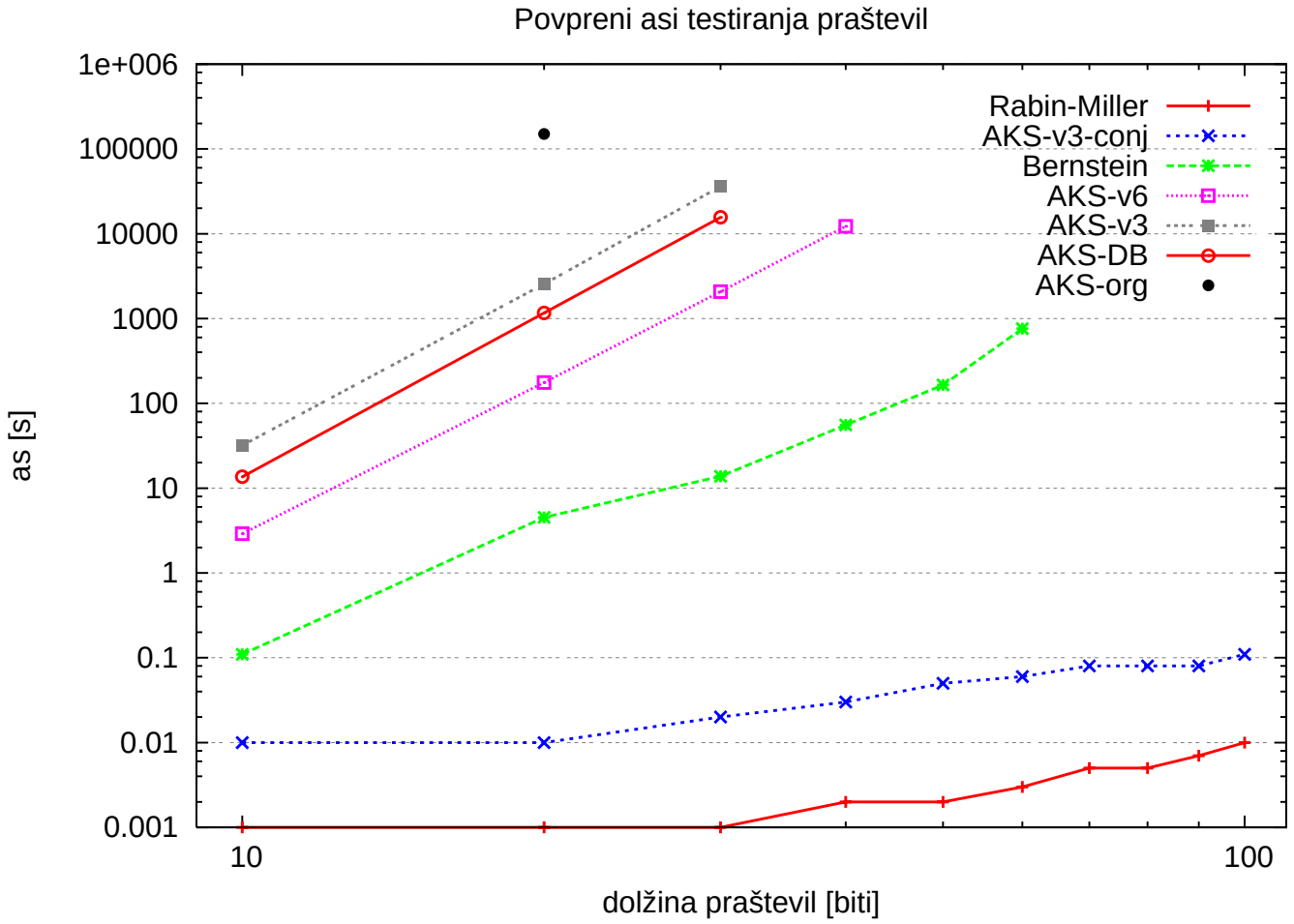
VHOD: število $n \geq 1$.

1. **if** $(n = a^b,\ a, b \in \mathbb{N},\ b > 1)$ **then** zaključi("sestavljeno število")
2. Pošči najmanjši r, da velja $o_r(n) > 4 \log^2 n$.
3. **if** $(1 < gcd(a, n) < n$ za kak $a \leq r)$ **then**
   zaključi("sestavljeno število")
4. **if** $(n \leq r)$ **then** zaključi("praštevilo")
5. **for** $a := 1, \ldots, \lfloor 2\sqrt{\phi(r)} \log n \rfloor$ **do**
   if $((X + a)^n \not\equiv X^n + a \pmod{X^r - 1, n})$ **then**
   zaključi("sestavljeno število")
6. Zaključi("praštevilo").

Izboljšave AKS in sorodni algoritmi

- verziji 3 in 6
- Bernsteinov algoritem s pričakovano polinomsko časovno zahtevnostjo
- Lenstra-Pomerancev algoritem z dokazano časovno zahtevnostjo $\mathcal{O}^{\sim}(\log^6 n)$
- Berrizbeitiov deterministični algoritem (malo hitrejši od AKS verzije 6, a ne deluje za čisto vsa števila)
- algoritem, ki temelju na nedokazani "domnevi 5" v originalnem članku (izjemno hiter)

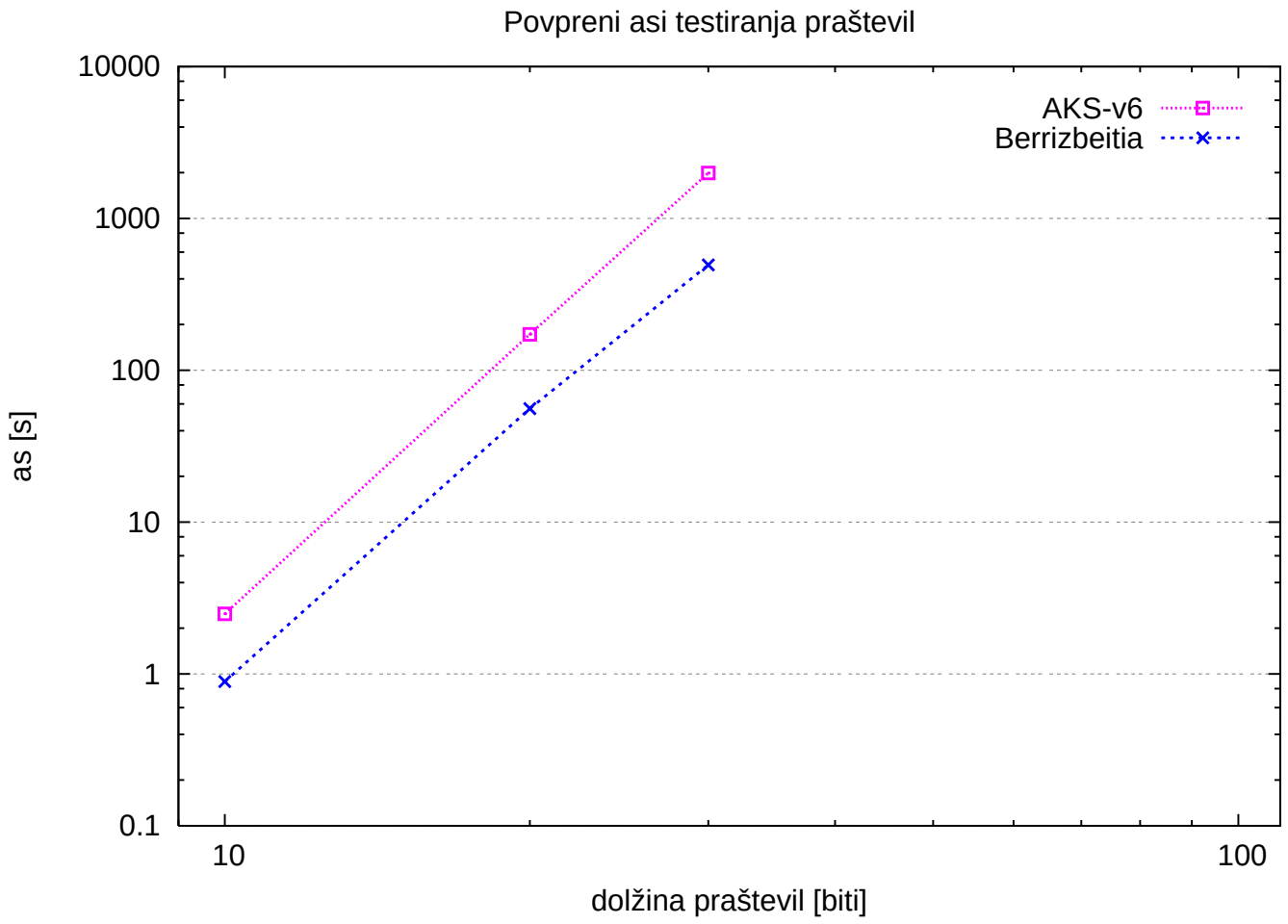
Testiranje srednjih praštevil (10-100 bitov)



Eksponent k v $\mathcal{O}(\log^k n)$

Algoritmi						
RM	AKS-v3-conj	Bernstein	AKS-v6	AKS-v3	AKS-DB	AKS-org
1.29	1.27	4.92	6.02	6.39	6.41	-

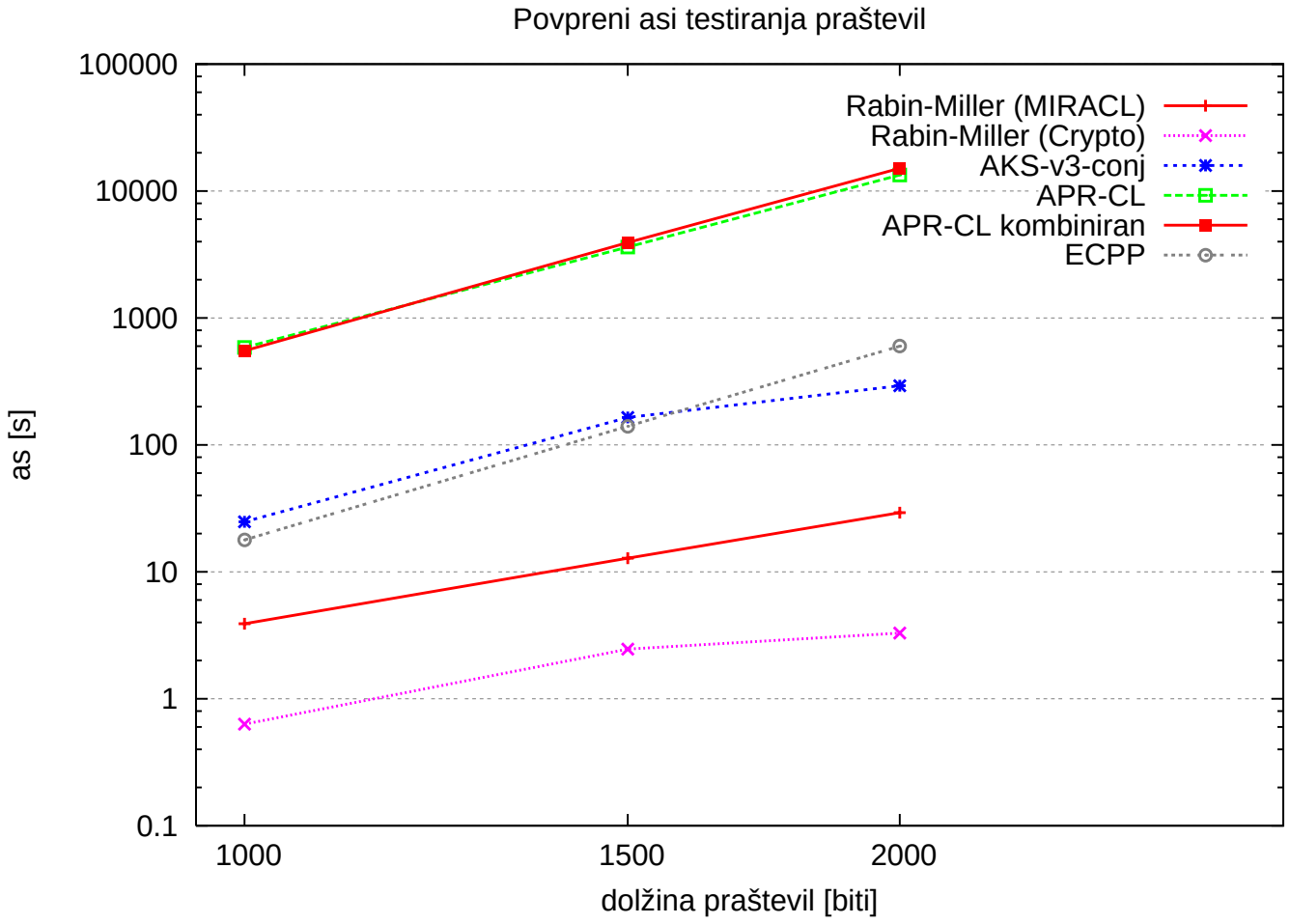
Testiranje srednjih praštevil (10-100 bitov) primernih za Berrizbetiov algoritem



Eksponent k v $\mathcal{O}(\log^k n)$

Algoritmi	
`AKS-v6`	`Berrizbeitia`
6.08	5.75

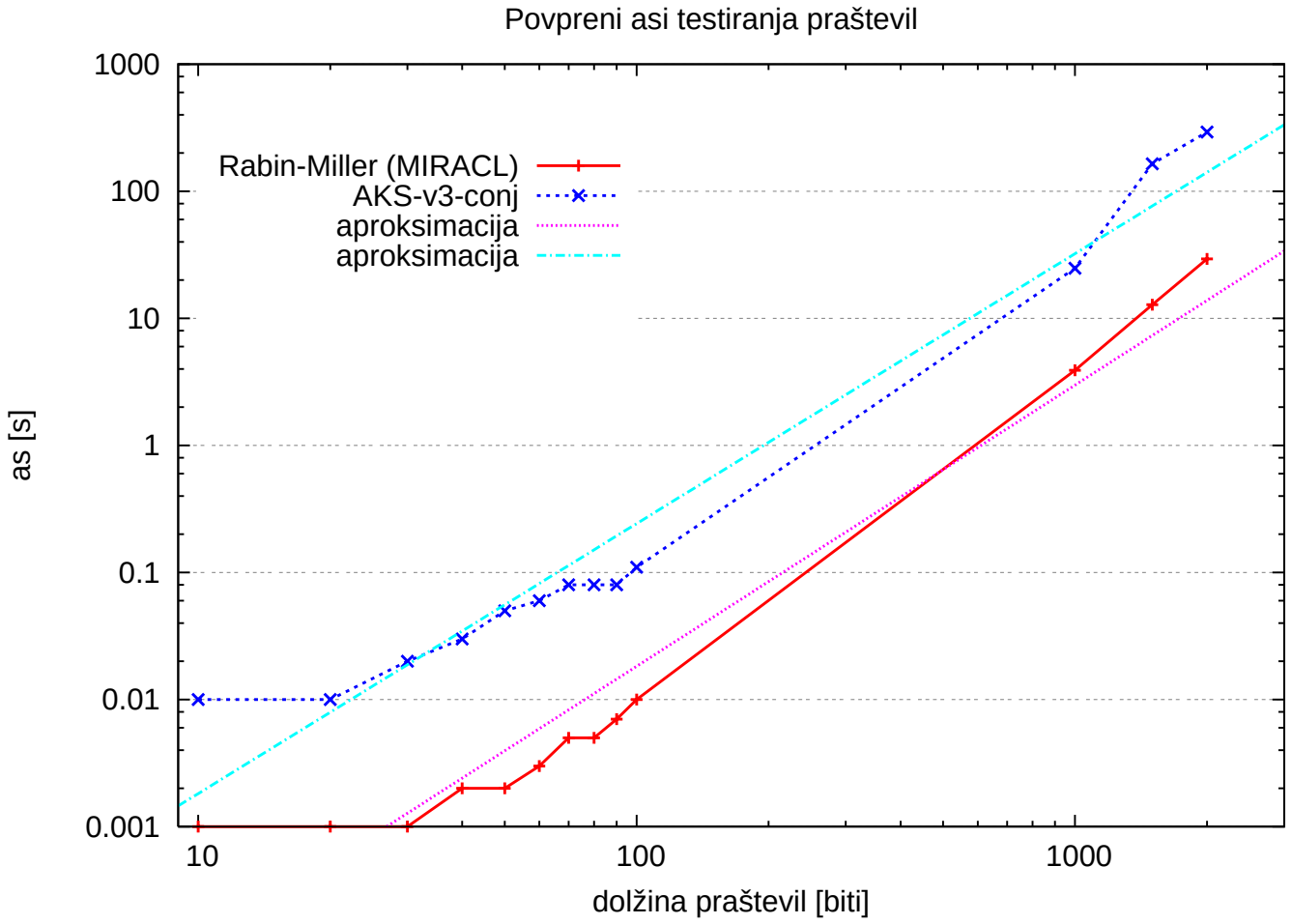
Testiranje velikih praštevil



Eksponent k v $\mathcal{O}(\log^k n)$

Algoritmi					
`RM` (MIRACL)	`RM` (Crypto)	`AKS-v3-conj`	VFYPR (le `APR-CL`)	VFYPR (kombiniran)	`ECPP`
2.91	2.39	3.56	4.51	4.77	5.07

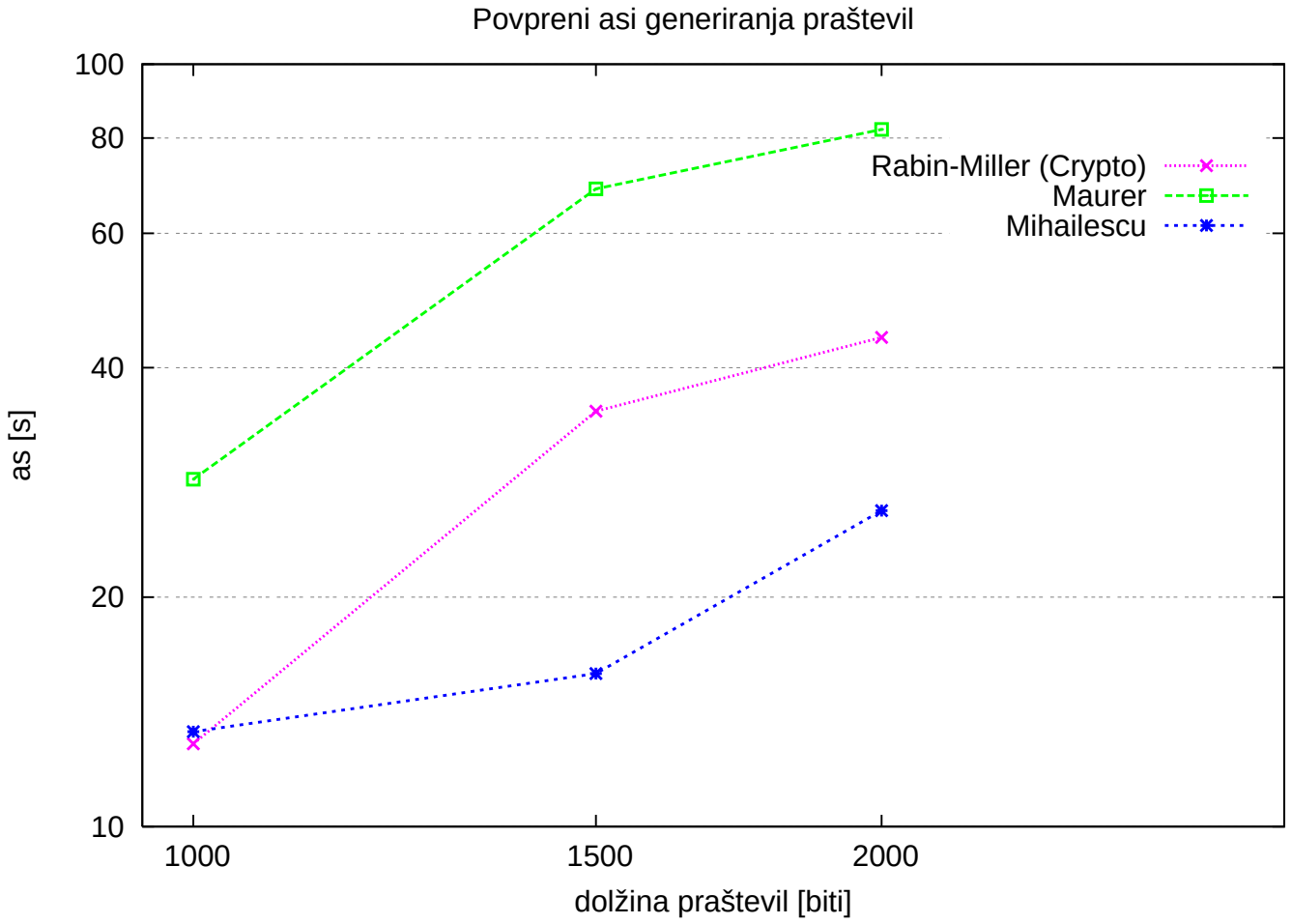
Združeni rezultati testiranja praštevil



Eksponent k v $\mathcal{O}(\log^k n)$

Algoritmi	
`RM` (MIRACL)	`AKS-v3-conj`
2.21	2.12

Generiranje velikih praštevil



Eksponent k v $\mathcal{O}(\log^k n)$

Algoritmi		
`RM` (Crypto)	`Maurer`	`Mihailescu`
1.77	1.52	0.96

Komentar rezultatov