

Cover Page



Universiteit Leiden



The handle <http://hdl.handle.net/1887/20880> holds various files of this Leiden University dissertation.

Author: Duong, Hoang Dung

Title: Profinite groups with a rational probabilistic zeta function

Issue Date: 2013-05-14

Chapter 6

Miscellaneous

From Theorem 1.2.2, Theorem 1.2.6, Theorem A and Theorem C, we obtain the following.

Theorem 6.0.2. *Let G be a finitely generated profinite group and S a finite simple group. Assume that almost every composition factor of G is isomorphic to S . Then $P_G(s)$ is rational if and only if $G/\text{Frat}(G)$ is a finite group.*

We would like to ask whether the conjecture holds if we replace the simple group S in Theorem 6.0.2 by a finite set $\mathcal{F}$ of simple groups. The problem is not easy even in the case $\mathcal{F}$ is of cardinality 2. In the first section, we give some examples showing difficulties for this situation. However, there are some cases in which the conjecture holds, as can be seen in the second section.

6.1 Examples

In this section, we will give some examples showing that our techniques are not effective in the general case.

Example 1 In this example, we consider the group G such that almost every composition factor of G is either an alternating group $\text{Alt}(m)$ or isomorphic to a projective special linear group $\text{PSL}(n, p)$. We will show that we cannot deduce the finiteness of $\pi(G)$ by our techniques.

Assume that $P_G(s)$ is factorized as

$$P_G(s) = \prod_{i \in J} P_i(s)$$

where J is the set of indices i such that the chief factor G_i/G_{i+1} is non-Frattini and Γ the set of the simple groups S_i with $i \in J$. Let I be the set of indices $i \in J$ such that S_i is either an alternating group or a projective special linear group, and let Γ^* be the set of simple groups such that $S_i \in \Gamma$ with $i \in I$. By our assumption, the Dirichlet series $A(s) = \prod_{i \in I} P_i(s)$ is rational, and hence $\pi(A(s))$ is finite. Assume that $p = 5$ does not belong to $\pi(A(s))$, as in Step 1 in Section 2.6.1. We need to prove that 5 is actually in $\pi(A(s))$ to obtain a contradiction. Let

$$\mathcal{S} = \{S \in \Gamma^* : 5 \in \pi(P_i(s))\}, r := \min\{r_i : S_i \in \mathcal{S}\} \text{ and } I^* := \{i \in I : r_i = r \text{ and } S_i \in \mathcal{S}\}$$

As in our process described in Section 2.6, we consider Λ the set of positive integers divisible by 5, and let $\beta \in \Lambda$ be minimal with the properties that $v_5(\beta) = r$ and $b_{i,\beta} \neq 0$ for some $i \in I$, i.e., β is a useful index for a group L_i with $i \in I$. At this step, we need to show that $b_{i,\beta} < 0$ for all i such that $b_{i,\beta} \neq 0$. However, if $S_i \cong \text{Alt}(3.5.11)$ then

$$P_i(s) = 1 - \frac{3.5.11}{(3.5.11)^{r_i s}} + \dots$$

while if $S_j \cong \text{PSL}(2, 11)$ then

$$P_j(s) = 1 - \frac{22}{11^{r_j s}} + \frac{165}{(3.5.11)^{r_j s}} + \dots$$

In this case, $\beta = 3.5.11$, but $b_{i,\beta} < 0$ while $b_{j,\beta} > 0$. Thus, we can not conclude that

$$c_\beta = \sum_{\substack{i \in I^* \\ r_i = r}} b_{i,\beta}$$

is different from 0. Therefore, we cannot conclude that 5 is in fact in $\pi(A(s))$, even though $5 \in \pi(G)$. Hence, we cannot conclude that $\pi(G)$ is a finite set.

Example 2 In this example, we consider the group G in which both $\text{PSL}(3, 3)$ and $\text{PSL}(12, 2)$ appear infinitely many times as composition factors in non-Frattini chief factors of G . We

will show that when the characteristics of simple groups of Lie type are different, then our techniques are not effective.

Assume in addition that $\pi(G)$ is finite. We need to prove the final step to deduce the finiteness of $G/\text{Frat}(G)$. As above, the product

$$A(s) = \prod_{i \in I} P_i(s)$$

is rational. We would like to deduce the emptiness of the set I . We will use reduction maps in Lemma 1.2.5 to simplify the product $A(s)$. We choose the prime $p = 2$ and so the product

$$\prod_{i \in I} P_i^{(2)}(s)$$

is still rational. At this step, normally we will look for a positive integer w with some additional properties, such that we can use Proposition 2.4.3 to obtain that the following product

$$\prod_{i \in I} \left(1 + \frac{b_{i,w^{r_i}}}{(w^{r_i})^s} \right), \text{ where } b_{i,w^{r_i}} < 0$$

is still rational. From that, we can then use the Corollary of the Skolem-Mahler-Lech Theorem. However, if $S_i \cong \text{PSL}(3,3)$ then

$$P_i^{(2)}(s) = 1 - \frac{26}{13^{r_i s}} + \frac{117}{(3^2 \cdot 13)^{r_i s}}$$

while if $S_i \cong \text{PSL}(12,2)$ then

$$P_i^{(2)}(s) = 1 - \frac{3^2 \cdot 5 \cdot 7 \cdot 13}{(3^2 \cdot 5 \cdot 7 \cdot 13)^{r_i s}} + \dots$$

In this situation, if we choose w in the set Λ of odd positive integers divisible by 3^2 and 13 such that $v_3(w) = 2$ and $v_{13}(w) = 1$, then if w would be $3^2 \cdot 13$. So $b_{i,w^{r_i}} = 117 > 0$. Thus, if we could reduce $A(s)$ to the product

$$\prod_{i \in I} \left(1 + \frac{b_{i,w^{r_i}}}{(w^{r_i})^s} \right)$$

we still can't apply the Skolem-Mahler-Lech Theorem since not all $b_{i,w^{r_i}}$ are negative.

6.2 Mixing up some families of simple groups

In this section, we will give a proof of the following theorem.

Theorem D. *Let G be a finitely generated profinite group of which almost every composition factor is isomorphic to either a sporadic group, or a projective special linear group $\text{PSL}(2, p)$ for some prime $p \geq 5$, or an alternating group $\text{Alt}(n)$ where n is either a prime or a power of 2. If $P_G(s)$ is rational then $G/\text{Frat}(G)$ is a finite group.*

We will use the techniques as in Chapter 4 and Chapter 5. We will focus on the smallest useful index in the monolithic group associated to a nonabelian composition factor $S \in \Gamma^*$. Descriptions of such useful indices when S is $\text{PSL}(2, p)$ or sporadic are included in Chapters 4 and 5. We now focus on the alternating groups $\text{Alt}(n)$ when n is either a prime or a power of 2.

When $n = p$ is a prime number, $\text{Alt}(p)$ has a maximal subgroup $M = \text{Alt}(p-1)$ of index p , and similarly for $\text{Sym}(p)$.

6.2.1 Maximal subgroups in alternating groups $\text{Alt}(2^t)$

Let X be an almost simple group whose socle is $\text{Alt}(n)$ where $n = 2^t$ is a power of 2, with $t \geq 3$. So either $X = \text{Alt}(n)$ or $X = \text{Sym}(n)$.

Let M be a maximal subgroup of X such that M contains a Sylow 2-subgroup of X . By Liebeck and Saxl ([LS85]), the group M is of either intransitive type or imprimitive type unless $n = 8$ and $X = \text{Alt}(8)$.

- In case M is of intransitive type, i.e., $M = (S_k \times S_{n-k}) \cap X$ with $1 \leq k < n/2$, then

$$|X : M| = \binom{n}{k}.$$

Let $n = \sum_i n_i 2^i$ and $k = \sum_i k_i 2^i$ be 2-adic expansions of n and k respectively, then applying Lucas' Theorem gives us

$$|X : M| = \binom{n}{k} \equiv \prod_i \binom{n_i}{k_i} \equiv 0 \pmod{2}$$

since $n_i = 0$ for all but $i = t$. Therefore M is always of even index in X , a contradiction. Hence M is not intransitive.

- In case M is of imprimitive type, i.e., $M = (S_a \wr S_b) \cap X$ where $ab = 2^t, a > 1, b > 1$, then M has index

$$w(a, b) = \frac{(2^t)!}{(a!)^b \cdot b!}.$$

Notice that $w(a, b)$ is always odd because of the following. For a given integer n , let $n = a_0 + a_1p + \cdots + a_dp^d$ be the p -adic expansion of n where p is a prime and $0 \leq a_j \leq p-1$ for each j , $a_d \neq 0$. Let $S_p(n) = a_0 + \cdots + a_d$, then Legendre's formula gives us

$$v_p(n!) = \frac{n - S_p(n)}{p-1}.$$

Now in this case $n = 2^t$, then $p = 2, a_t = 1$ and $a_k = 0$ for all $k \neq t$. So $S_2(n) = 1$. We have that $v_2(n!) = 2^t - 1$. Assume that $a = 2^u, b = 2^v$ then $v_2(a) = 2^u - 1$, $v_2(b) = 2^v - 1$ so that

$$v_2((2^u!)^{2^v}) = (2^u - 1)2^v.$$

Then

$$v_2((2^u!)^{2^v} \cdot 2^{v!}) = (2^u - 1)2^v + 2^v - 1 = 2^{u+v} - 1 = 2^t - 1.$$

Hence $w(a, b)$ is always odd.

- In case $n = 8$ and $X = \text{Alt}(8)$ then $M = 2^3 : \text{PSL}(3, 2)$. So $|X : M| = 3 \cdot 5$.

Lemma 6.2.1. [Mar02, Lemma 2.1] Assume that $m = ab \geq 8, a, b \geq 2$. Then

$$w(a, b) = \frac{m!}{a!^b \cdot b!}$$

is smallest when b is the smallest prime divisor of n .

Proof. We may assume that $a \geq b$ since if $b > a$ then

$$b!^{a-1} = a!^{a-1}(a+1)^{a-1} \cdots b^{a-1} > a!^{a-1}a^{(b-a)(a-1)}.$$

In addition, we have that $a^{a-1} > 1 \cdot 2 \cdots a = a!$ and so

$$b!^{a-1} > a!^{a-1}a!^{b-a} = a!^{b-1}$$

which implies that

$$b!^a \cdot a! > a!^b \cdot b! \Rightarrow \frac{m!}{a!^b \cdot b!} > \frac{m!}{b!^a \cdot a!}.$$

Assume now that $m = a_1 b_1 = a_2 b_2$ with $b_1 \leq a_1, b_2 \leq a_2$. If $b_1 \leq b_2$ then $a_1 \geq a_2$ and

$$\begin{aligned}
a_1!^{b_1} \cdot b_1! &\geq a_2!^{b_1} (a_2 + 1)^{b_1} \cdots a_1^{b_1} b_1! \geq a_2!^{b_1} a_2^{(a_1 - a_2)b_1} b_1! \quad (\text{since } a_1 \geq a_2) \\
&= a_2!^{b_1} b_1! (a_2^{a_2})^{\frac{b_1}{a_2}(a_1 - a_2)} = a_2!^{b_1} b_1! (a_2^{a_2 - 1} a_2)^{\frac{b_1}{a_2}(a_1 - a_2)} \\
&\geq a_2!^{b_1} b_1! (a_2! b_2)^{\frac{b_1}{a_2}(a_1 - a_2)} = a_2!^{b_1} b_1! (a_2! b_2)^{b_2 - b_1} \quad (\text{since } a_2 \geq b_2 \text{ and } a_1 b_1 = a_2 b_2) \\
&\geq a_2!^{b_2} b_1! (b_1 + 1) \cdots b_2 = a_2!^{b_2} b_2! \quad (\text{since } b_2 \geq b_1)
\end{aligned}$$

and hence

$$\frac{m!}{a_1!^{b_1} \cdot b_1!} \leq \frac{m!}{a_2!^{b_2} \cdot b_2!}$$

□

In particular, when $n = 2^t$, then $w(2^{t-1}, 2)$ is the smallest among $w(a, b)$ with $n = ab$, $a > 1, b > 1$.

Theorem 6.2.2. *Let L be a monolithic primitive group with socle is $(\text{Alt}(2^t))^r$. Let*

$$w = \begin{cases} (2^t)! / ((2^{t-1}!)^2 \cdot 2!) & \text{if } t > 3, \\ 3 \cdot 5 & \text{if } t = 3. \end{cases}$$

Let q be the largest prime less than 2^t if $t > 3$ and $q = 5$ otherwise. Then w^r is the smallest odd q -useful index for L .

6.2.2 The main result

Let G now be a finitely generated profinite group of which almost every nonabelian composition factor is isomorphic to either a sporadic group, or a projective special linear group $\text{PSL}(2, p)$ for some prime $p \geq 5$, or an alternating group $\text{Alt}(n)$ where n is either a prime or a power of 2. Assume in addition that $P_G(s)$ is rational.

We fix a descending normal series $\{G_i\}$ of G with the properties that $\bigcap G_i = 1$ and G_i/G_{i+1} is a chief factor of G/G_{i+1} . Let J be the set of indices i with G_i/G_{i+1} non-Frattini. Then by Section 2.1, the probabilistic zeta function $P_G(s)$ can be factorized as

$$P_G(s) = \prod_{i \in J} P_i(s)$$

where for each i , the finite Dirichlet series $P_i(s)$ is associated to the chief factor G_i/G_{i+1} . We have the following crucial result.

Proposition 6.2.3. *The set $\pi(G)$ is finite.*

Proof. Let Γ be the set of simple groups that appear as composition factors in non-Frattini chief factors of G . Let Γ^* be the subset of Γ containing simple groups $S_i \in \Gamma$ such that S_i is isomorphic to either a sporadic simple group, or $\text{PSL}(2, p)$ for some prime $p \geq 5$, or an alternating group $\text{Alt}(n)$ where n is either a prime or a power of 2.

Notice that for each simple group $S \in \Gamma^*$ which is not sporadic, either there is an odd prime r such that $S \cong \text{PSL}(2, r)$ or $S \cong \text{Alt}(r)$ or $S \cong \text{Alt}(2^t)$ for some $t \geq 3$. In the latter case, there is also an associated prime p_t , namely the largest prime less than 2^t . Notice also that for a given prime p , there are only finitely many numbers n such that p is the largest prime less than n , since for every large enough positive integer x , there is always a prime in the interval $[x, 6/5x]$ (see [Nag52]). Now we proceed as in Chapter 4 and 5.

Assume by contradiction that Γ^* is infinite. Let I be the set of indices i such that $S_i \in \Gamma^*$ and let $A(s) = \prod_{i \in I} P_i(s)$, $B(s) = \prod_{i \in I \setminus I^*} P_i(s)$. Since $\pi(P_G(s))$ is finite and by hypothesis, $\pi(B(s))$ is finite, it follows that $\pi(A(s))$ is finite. In particular, there is a prime $p > 71$ such that $p \notin \pi(A(s))$. We choose the prime number $p > 71$ since 71 is the largest prime dividing the order of a sporadic simple group, so if p divides some $|S_i|$ then S_i is either an alternating group or a projective special linear group. Set

$$I^* = \{i \in I : p \in \pi(P_i(s))\} \quad \text{and} \quad r = \min\{r_i : i \in I^*\}.$$

Let Λ be the set of all odd positive integers n such that n is divisible by p and is not divisible by any prime strictly larger than p . Notice that for each $i \in I^*$, there exists $\alpha \in \Lambda$ such that α is a useful index for L_i . Indeed, if $p \in \pi(P_i(s))$ then one of the following occurs:

- $S_i = \text{PSL}(2, p)$ and $(p(p \pm 1)/2)^{r_i}$ are useful indices for L_i .
- $S_i = \text{Alt}(p)$ and p^{r_i} is a useful index for L_i .
- $S_i = \text{Alt}(2^t)$ and $w(2^t, 2)$ is a useful index for L_i .

Choose $\alpha \in \Lambda$ minimal with the properties that there exists $i \in I^*$ such that $r_i = r$, and $v_p(\alpha) = r$ and α is a useful index for L_i . Notice that if $i \in I$ such that $b_{i,\alpha} \neq 0$ then $i \in I^*$,

and $r_i = r$ and α is the smallest odd p -useful index for L_i . It follows that $b_{i,\alpha} < 0$. Hence the coefficient c_α of $1/\alpha^s$ in $A(s)$ is

$$c_\alpha = \sum_{\substack{i \in I \\ r=r_i}} b_{i,\alpha} = \sum_{i \in I^*} b_{i,\alpha} < 0$$

which implies that $p \in \pi(A(s))$, a contradiction. Hence Γ^* . It follows that Γ is finite. Consequently, the set $\pi(G)$ is also finite. $\square$

Proof of Theorem D. Let $\mathcal{T}$ be the set of almost simple groups X such that there are infinitely many indices $i \in J$ with $X_i \cong X$, and let $I = \{i \in J : X_i \cong X\}$. Our assumptions combined with Proposition 2.6.3, imply that $J \setminus I$ is finite. In order to prove that J is finite, we need to prove that I is empty. Since $P_G(s)$ is rational, also $\prod_{i \in I} P_i(s)$ is rational. By Lemma 1.2.5, the product $\prod_{i \in I} P_i^{(2)}(s)$ is still rational. Notice that the set $\pi(\mathcal{T})$ of prime divisors of orders of simple groups S such that $S = \text{soc}(X)$ for some $X \in \mathcal{T}$ is finite. Let

$$q = \max\{p : p \in \pi(\mathcal{T})\}$$

and

$$\Lambda_q = \{i \in I : q \in \pi(P_i^{(2)}(s))\}.$$

Notice that if $q > 71$ and $i \in \Lambda_q$ then S_i is isomorphic to either $\text{Alt}(q)$ or $\text{Alt}(2^t)$, where q is the largest prime less than 2^t , or $\text{PSL}(2, q)$. Let

$$\begin{aligned} w &= \min\{x \in \mathbb{N} \mid x \text{ is odd, } v_q(x) = 1 \text{ and } b_{i,x^{r_i}} \neq 0 \text{ for some } i\} \\ &= \min\{x \in \mathbb{N} \mid x \text{ is odd, } v_q(x) = 1 \text{ and } b_{i,x^{r_i}} \neq 0 \text{ for some } i \in \Lambda_q\}. \end{aligned}$$

Note that if $i \in \Lambda_q$, and n is minimal with the properties that n is odd, $b_{i,n^{r_i}} \neq 0$ and $v_q(n) = 1$, then $b_{i,n^{r_i}} < 0$. So if $b_{i,n^{r_i}} \neq 0$ then $b_{i,n^{r_i}} < 0$. Moreover, by Proposition 2.4.3, we obtain the rational product

$$\prod_{i \in \Lambda_q} \left(1 + \frac{b_{i,w^{r_i}}}{(w^{r_i})^s}\right)$$

where $b_{i,w^{r_i}} \leq 0$ for each $i \in \Lambda_q$. By applying Corollary 2.5.5, we get that $\Lambda_q^* = \{i \in \Lambda_q \mid b_{i,w^{r_i}} \neq 0\}$ is finite, but this implies that $\Lambda_q = \emptyset$. Let

$$p = \max\{r : r \in \pi(\mathcal{T}) \setminus \{q\}\}$$

and

$$\Lambda_p = \{i \in I : p \in \pi(P_i^{(2)}(s))\}.$$

Again, by the same argument, we obtain that $\Lambda_p = \emptyset$. We continue this procedure until we reach the prime 71. Notice that we deal with both $\text{PSL}(2, 71)$, $\text{Alt}(71)$ and M by the prime 71. Now, with the same spirit, we deal with all remaining sporadic groups, alternating groups and $\text{PSL}(2, q)$ with $5 \leq q < 71$. Our process is described in order in the following table in which the first column stands for the primes r we use in order to deduce that $\Lambda_r = \emptyset$, the second column are simple groups S involved corresponding to the primes in the first column:

r	S
71	$\text{PSL}(2, 71), M, \text{Alt}(71)$
67	$\text{PSL}(2, 67), \text{Alt}(67), \text{Ly}$
61	$\text{Alt}(61), \text{Alt}(2^6)$
59	$\text{PSL}(2, 59), \text{Alt}(59)$
53	$\text{PSL}(2, 53), \text{Alt}(53)$
47	$\text{PSL}(2, 47), \text{Alt}(47), \text{BM}$
43	$\text{PSL}(2, 43), \text{Alt}(43), J_4$
41	$\text{PSL}(2, 41), \text{Alt}(41)$
37	$\text{PSL}(2, 37), \text{Alt}(37)$
31	$\text{PSL}(2, 31), \text{Alt}(31), \text{Alt}(2^5), \text{O}'\text{N}$
29	$\text{PSL}(2, 29), \text{Alt}(29), \text{Fi}'_{24}, \text{Ru}$
23	$\text{PSL}(2, 23), \text{Alt}(23), M_{23}, M_{24}, \text{Co}_2, \text{Co}_3, \text{Fi}_{23}$
19	$\text{PSL}(2, 19), \text{Alt}(19), J_1, J_3, \text{HN}, \text{Th}$
17	$\text{PSL}(2, 17), \text{Alt}(17), \text{He}$
13	$\text{PSL}(2, 13), \text{Alt}(13), \text{Alt}(2^4), \text{Suz}, \text{Co}_1, \text{Fi}_{22}$
11	$\text{PSL}(2, 11), \text{Alt}(11), M_{11}, M_{12}, M_{22}, \text{HS}, \text{McL}$
7	$\text{PSL}(2, 7), \text{Alt}(7), J_2$
5	$\text{PSL}(2, 5), \text{Alt}(5), \text{Alt}(2^3)$

□

6.2.3 Appendix

Table 6.2: Even numbers n with largest prime less than 71 and potential primes p such that $v_p(w) = 1$ where $w = n! / (m!)^t \cdot t!$

n	potential primes
10	7
12	7, 11
14	11, 13
16	11, 13
18	11, 13, 17
20	11, 13, 17, 19
22	13, 17, 19
24	13, 17, 19, 23
26	17, 19, 23
28	17, 19, 23
30	17, 19, 23, 29
32	17, 19, 23, 29, 31
34	19, 23, 29, 31
36	19, 23, 29, 31
38	23, 29, 31, 37
40	23, 29, 31, 37
42	23, 29, 31, 37, 41
44	23, 29, 31, 37, 41, 43
46	29, 31, 37, 41, 43
48	29, 31, 37, 41, 43, 47
50	29, 31, 37, 41, 43, 47
52	29, 31, 37, 41, 43, 47
54	29, 31, 37, 41, 43, 47, 53
56	29, 31, 37, 41, 43, 47, 53
58	31, 37, 41, 43, 47, 53
60	31, 37, 41, 43, 47, 53, 59
62	37, 41, 43, 47, 53, 59, 61
64	37, 41, 43, 47, 53, 59, 61
66	37, 41, 43, 47, 53, 59, 61
68	37, 41, 43, 47, 53, 59, 61, 67
70	37, 41, 43, 47, 53, 59, 61, 67
72	37, 41, 43, 47, 53, 59, 61, 67, 71

Table 6.3: Prime divisors of $|\text{PSL}(2, q)|$ for $q \leq 71$

q	$ \text{PSL}(2, q) $	Smallest odd useful index
71	$2^3 \cdot 3^2 \cdot 7 \cdot 71$	$5 \cdot 7 \cdot 71$
67	$2^2 \cdot 3 \cdot 11 \cdot 17 \cdot 67$	$3 \cdot 11 \cdot 67$
61	$2^2 \cdot 3 \cdot 5 \cdot 31 \cdot 61$	$31 \cdot 61$

59	$2^2 \cdot 3 \cdot 5 \cdot 29 \cdot 59$	$29 \cdot 59$
53	$2^2 \cdot 3^2 \cdot 13 \cdot 53$	$3^3 \cdot 53$
47	$2^4 \cdot 3 \cdot 23 \cdot 47$	$23 \cdot 47$
43	$2^2 \cdot 3 \cdot 7 \cdot 11 \cdot 43$	$3 \cdot 7 \cdot 43$
41	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 41$	$3 \cdot 7 \cdot 41$
37	$2^2 \cdot 3^2 \cdot 19 \cdot 37$	$19 \cdot 37$
31	$2^5 \cdot 3 \cdot 5 \cdot 31$	$3 \cdot 5 \cdot 31$
29	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 29$	$29 \cdot 7$
23	$2^3 \cdot 3 \cdot 11 \cdot 23$	$11 \cdot 23$
19	$2^2 \cdot 3^2 \cdot 5 \cdot 19$	$19 \cdot 3$
17	$2^4 \cdot 3^2 \cdot 17$	$3^2 \cdot 17$
13	$2^2 \cdot 3 \cdot 7 \cdot 13$	$7 \cdot 13$
11	$2^2 \cdot 3 \cdot 5 \cdot 11$	11
7	$2^3 \cdot 3 \cdot 7$	7
5	$2^2 \cdot 3 \cdot 5$	5

