Periodica Mathematica Hungarica Vol. 43 (1–2), (2001), pp. 191–198

THE EXPECTED NUMBER OF RANDOM ELEMENTS TO GENERATE A FINITE ABELIAN GROUP

Carl Pomerance (Murray Hill)

Dedicated to Professor András Sárközy on the occasion of his 60th birthday

Abstract

Suppose G is a finite abelian group with minimal number of generators r. It is shown that the expected number of elements from G (chosen independently and with the uniform distribution) so that the elements chosen generate G is less than $r + \sigma$, where $\sigma = 2.118456563\ldots$. The constant σ is explicitly described in terms of the Riemann zeta-function and is best possible.

Introduction

If one chooses random elements from a finite group G independently, and with the uniform distribution, how many should one expect to pick until the elements chosen generate the group? From [3], one may answer this question asymptotically for the symmetric group S_n and the alternating group A_n. In that paper, it is shown that two randomly chosen elements from S_n generate either S_n or A_n with probability $1 - o(1)$ as $n \to \infty$. Thus, the expected number to generate S_n is $2.5 + o(1)$ as $n \to \infty$, and if one chooses from A_n, the expected number to generate is $2 + o(1)$. It was also conjectured in [3] that for any finite simple group G, the probability that two randomly chosen elements generate G is $1 - o(1)$ as $|G|$, the order of G, tends to infinity. The proof of this conjecture was completed in [9], and so it follows that the expected number of elements to generate a finite nonabelian simple group is $2 + o(1)$.

In [1], the expected number of random elements to generate a group G is worked out for all groups of order < 16. In addition, it is shown, in principle, how one could work out this expectation for any finite group which is a direct product of p-groups. This includes of course all finite abelian groups.

In this note we carry out the calculation of this expectation for all finite abelian groups, and so discover a perhaps unexpected consequence: the expectation minus the minimal number of generators is bounded. That is, there is a universal

Mathematics subject classification number: 20P05.

Key words and phrases: finite abelian group, finite nilpotent group, expected number of generators, Riemann zeta-function.

0031-5303/01/$5.00

Akadémiai Kiadó, Budapest
Kluwer Academic Publishers, Dordrecht

constant $\sigma = 2.118456563\ldots$, such that the expected number of random elements to generate a finite abelian group with minimal number of generators r is $< r + \sigma$. The number σ is explicitly described in terms of the Riemann zeta-function and is best possible. We also give the corresponding result for various subclasses of finite abelian groups: groups with fixed minimal number of generators and groups $\mathbf{Z}_n^*$, the multiplicative group of units in the ring $\mathbf{Z}_n$.

It was noted in [7] that the expected number of independent, uniform random choices from the cyclic multiplicative group $G = \mathbf{Z}_p^*$, where p is a prime, to generate G, is $O(1)$, uniformly for all primes p. The argument is easy. For each prime q dividing $p-1$, the order of G, the probability that *two* independent, uniform randomly chosen elements both lie in the subgroup of index q is q^{-2}. Thus, the probability that the two elements do not already generate G is the product of $1-q^{-2}$ as q runs over the prime factors of the order of G. This product is larger than $1/\zeta(2) = 6/\pi^2$, where ζ is the Riemann zeta-function. Since this probability is bounded above zero, the expected number of choices is uniformly bounded, in fact less than $2\zeta(2) = \pi^2/3$. This argument works for any finite cyclic group. It is shown below that the "best" constant here is

$$2 + \sum_{j=2}^{\infty} (1 - \zeta(j)^{-1}) = 2.7052111401\ldots.$$

That is, the expected number of random choices to generate a finite cyclic group G is always smaller than this number, but no smaller number has this property. The numerical calculation of this sum, like all calculations in this note, was performed with Mathematica.

The fact that the expected number of random choices of elements to generate a cyclic group is $O(1)$ has some consequences for primality testing. It has been known since Lucas that if you have the complete prime factorization of $p-1$, the prime p can be proved prime via the exhibition of a primitive root (a cyclic generator of $\mathbf{Z}_p^*$). There is no known fast and deterministic method for finding a primitive root, but the probabilistic method of searching randomly is expected to succeed in $O(\log\log p)$ tries, a result that is best possible for infinitely many primes p. However, one can equally prove primality using a set of generators, and so one can reduce the effort to just $O(1)$ random picks from the group.

The problem of randomly generating the cyclic group $\mathbf{Z}_{p^e}^*$, for p an odd prime, is considered in [11]. The probability that K choices of elements do not yet generate is computed, as well as the probability that K choices generate only a small subgroup. These results are used in a zero-knowledge protocol to convince someone that you possess the prime factorization of an RSA modulus n.

In the case of a dimension r vector space over the prime finite field $\mathbf{F}_p$, we may consider the vector space as a finite abelian group under vector addition. The process of generating this group may be thought of as passing a series of tests. First we must choose a nonzero vector. Next, a vector not in the subspace generated by it must be chosen. And so on. If the dimension of the subspace already generated is j and $j < r$, then the probability of choosing a vector not in this subspace is

$1 - p^{j-r}$, so that the expected number of choices to choose such an element is $(1-p^{j-r})^{-1}$. Since expectation is additive, we deduce that the expected number of random choices to generate the full vector space is

$$\sum_{l=1}^{r}(1-p^{-l})^{-1} = r + \sum_{l=1}^{r}(p^l - 1)^{-1}.$$

This argument is well known. It is mentioned in [2], for example, in the case of vector spaces over the field of 2 elements.

The problem of choosing random elements to generate a class group is considered in algorithms to compute class groups and class numbers. This has applications to the rigorous study of factoring, for example see [8].

For a finite group G, let $r(G)$ denote the minimal number of generators of G. Also let $E(G)$ denote the expected number of elements from G, independently chosen with the uniform distribution, to generate G. Clearly $E(G) \geq r(G)$. Let $e(G) = E(G) - r(G)$, the *excess* of G. In every case considered above, $e(G) = O(1)$, uniformly. It is tempting to conjecture that this holds for all finite groups G, and I originally made such a conjecture. However, Alexander Lubotzky has pointed out to me that this is not true. In his paper [6] with Kantor, it is shown (see Example 2 on page 82) that for n sufficiently large, an $n!/8$-fold direct product of the alternating group A_n with itself is generated by two elements, yet the probability that $\lfloor\sqrt{n}\rfloor$ randomly chosen elements generate the group tends to 0 as $n \to \infty$. One concludes that the excesses for the groups in this sequence are unbounded. So the numbers $e(G)$ are unbounded in general, but they remain uniformly bounded for finite abelian groups, for finite simple groups, and for the symmetric groups. As mentioned in the remarks at the end of the paper, the same is true for finite nilpotent groups, and in fact the supremum of $e(G)$ over this class is the same as for the finite abelian groups, namely the number σ. It remains an interesting problem to discover for which classes of finite groups, the numbers $e(G)$ remain bounded. Does $e(G)$ remain bounded for finite solvable groups? Another problem: given some bound B, one can ask for a description of those finite groups G for which $e(G) \leq B$, and an estimation for the minimal order of a group G with $e(G) > B$. By tightening the estimates in the example in [6] one sees that this minimal order is $\leq \exp(\exp((1+o(1))B\log B))$. Is this best possible?

Theorem

For a finite abelian group G (with operation $+$) and for p a prime dividing $|G|$, the order of G, let $r_p = r_p(G)$ denote the p-rank of G. That is, r_p is the dimension of the $\mathbf{F}_p$-vector space G/pG. We let $r = r(G)$ be the maximum of r_p for $p \mid |G|$. Then G has a set of generators of cardinality r, and no smaller set can generate G.

The following theorem computes the excess $e(G)$ $(= E(G) - r(G))$ for any finite abelian group G. All of our other results will follow as corollaries.

THEOREM. *For any finite abelian group G we have*

$$e(G) = \sum_{j=0}^{\infty} \left(1 - \prod_{p \mid |G|} \prod_{i=1}^{r_p} (1 - p^{-(r-r_p+j+i)}) \right).$$

PROOF. We first consider the situation when G is a finite abelian p-group for some prime p. Thus, $r = r_p$. For the sequence $a_1, a_2, \ldots, a_l$ of elements of G, consider the chain of subgroups

$$(1) \qquad pG \subset pG + \langle a_1 \rangle \subset pG + \langle a_1, a_2 \rangle \subset \ldots \subset pG + \langle a_1, a_2, \ldots, a_l \rangle.$$

For $G = \langle a_1, a_2, \ldots, a_l \rangle$ to be true it is necessary and sufficient that the above chain of subgroups have exactly $r = r_p$ strict inclusions. Indeed, the elements $a_1, a_2, \ldots, a_l$ generate G if and only if the cosets $a_1 + pG, a_2 + pG, \ldots, a_l + pG$ generate G/pG. One direction is obvious. To see the other, let H be the subgroup of G generated by $a_1, \ldots, a_l$. We are assuming that $H + pG = G$ and we wish to show that this forces $H = G$. Say the largest order of an element in G is p^m. If $m = 1$, then $pG = \{0\}$, so the claim is clear. Suppose it is true for $m = n$, and assume, by way of induction, that $m = n + 1$. We have that pH is a subgroup of pG, that $pH + p(pG) = pG$ and that the largest order of an element in pG is p^m. Thus, by the induction hypothesis, $pH = pG$. Then $G = H + pG = H + pH = H$, and the assertion is proved.

We define some probabilities. For $j \geq 0$, let $P_{r,j}(p)$ be the probability that the number l in our chain (1) where we first generate G is less than or equal to $r + j$. Alternatively, since G/pG is isomorphic to $\mathbf{F}_p^r$, we have that $P_{r,j}(p)$ is the probability that $r + j$ vectors randomly chosen from $\mathbf{F}_p^r$ span this vector space. Placing these vectors as rows in a matrix, we are asking for the probability that a random $(r+j) \times r$ matrix over $\mathbf{F}_p$ has full rank r; that is, that the r column vectors in $\mathbf{F}_p^{r+j}$ are linearly independent. By the argument mentioned in the introduction, this probability is easily computed; we have

$$(2) \qquad P_{r,j}(p) = \prod_{i=1}^{r} \left(1 - p^{-(j+i)} \right).$$

(The formula (2) is essentially the same as Lemma 4 in [1].)

Consider now the general case of a finite abelian group G with minimal number of generators r. We write G as the direct product of p-groups G_p, with p-rank r_p, where p runs over the prime factors of $|G|$. We have $r = \max\{r_p : p \mid |G|\}$. Let P_j be the probability that the number l in our chain where we first generate G is less than or equal to $r + j$. That is, P_j is the probability that $r + j$ randomly chosen elements from G generate G. Then the expected value of l is

$$
\begin{aligned}
E(G) &= rP_0 + \sum_{j=1}^{\infty}(r+j)(P_j - P_{j-1}) \\
&= r\left(P_0 + \sum_{j=1}^{\infty}(P_j - P_{j-1})\right) + \sum_{j=1}^{\infty} j(P_j - P_{j-1}) \qquad (3) \\
&= r + \sum_{j=1}^{\infty} j(P_j - P_{j-1}).
\end{aligned}
$$

Since G is a product of the various groups G_p, we have from (2) that

$$
P_j = \prod_{p \mid |G|} P_{r_p, r-r_p+j}(p) = \prod_{p \mid |G|} \prod_{i=1}^{r_p} \left(1 - p^{-(r-r_p+j+i)}\right). \qquad (4)
$$

So, using (3) and (4), we have

$$
\begin{aligned}
E(G) &= r + \sum_{j=1}^{\infty} j(P_j - P_{j-1}) \\
&= r + \lim_{n\to\infty}\left(nP_n - \sum_{j=0}^{n-1} P_j\right) \\
&= r + \lim_{n\to\infty}\left(n\prod_{p\,|\,|G|}\prod_{i=1}^{r_p}(1-p^{-(r-r_p+n+i)}) - \sum_{j=0}^{n-1}\prod_{p\,|\,|G|}\prod_{i=1}^{r_p}(1-p^{-(r-r_p+j+i)})\right) \\
&= r + \lim_{n\to\infty}\left(n - \sum_{j=0}^{n-1}\prod_{p \mid |G|}\prod_{i=1}^{r_p}(1-p^{-(r-r_p+j+i)})\right) \\
&= r + \sum_{j=0}^{\infty}\left(1 - \prod_{p \mid |G|}\prod_{i=1}^{r_p}(1-p^{-(r-r_p+j+i)})\right).
\end{aligned}
$$

This concludes the proof of the theorem.

Corollaries

From the theorem we obtain the following corollaries.

COROLLARY 1. *For r a positive integer, let*

$$e_r = \sup\{e(G) : G \text{ a finite abelian group, } r(G) = r\}.$$

Then

$$e_r = 1 + \sum_{j=1}^{\infty}\left(1 - \prod_{l=1}^{r}\zeta(j+l)^{-1}\right).$$

PROOF. Of all finite abelian groups G with $r(G) = r$ and with $|G|$ having exactly k distinct prime factors, it is clear from the theorem that the largest possible value of $e(G)$ is

$$\sum_{j=0}^{\infty}\left(1-\prod_{\text{first } k \text{ primes } p}\prod_{l=1}^{r}(1-p^{-(j+l)})\right).$$

As k increases, so does $e(G)$. Further, for a fixed value of $j \geq 1$, the double product has limit $\prod_{l=1}^{r}\zeta(j+l)^{-1}$ as $k \to \infty$, while for $j = 0$, the double product has limit 0. This completes the proof.

COROLLARY 2. *Let*

$$\sigma = \sup\{e(G) : G \text{ a finite abelian group}\}, \quad c = \prod_{j=2}^{\infty}\zeta(j)^{-1}.$$

Then

$$\sigma = \lim_{r\to\infty} e_r = 1 + \sum_{j=2}^{\infty}\left(1 - c\prod_{l=2}^{j-1}\zeta(l)\right) = 2.118456563\ldots.$$

We remark that the constant c plays another role with finite abelian groups. Let $A(x)$ be the number of non-isomorphic abelian groups with order at most x. Then $A(x) = c^{-1}x + O(x^{1/2})$, a result due to Erdős and Szekeres [4]. See [5, page 439], for subsequent developments with the problem.

An important special case is the group $\mathbf{Z}_n^*$, the multiplicative group of residues modulo n. For $n > 2$, we have $r = r_2$ for this group. In addition, if we let $\omega(n)$ denote the number of distinct prime factors of n, we have

$$r_2 = \begin{cases} \omega(n), & n \equiv 1 \pmod 2 \\ \omega(n) - 1, & n \equiv 2 \pmod 4 \\ \omega(n), & n \equiv 4 \pmod 8 \\ \omega(n) + 1, & n \equiv 0 \pmod 8. \end{cases}$$

In the latter two cases we have $r_2 > r_p$ for every odd prime p dividing the order of $\mathbf{Z}_n^*$. In these cases, our Theorem gives a smaller value for the supremum of the excess:

COROLLARY 3. *Let*

$$\sigma_2 := \sup\{e(G) : G \text{ is a finite abelian group and } r_2(G) > r_p(G) \text{ for every odd prime } p\}.$$

Then

$$\sigma_2 = \sum_{j=1}^{\infty}\left(1 - (1-2^{-j})c\prod_{l=2}^{j}\zeta(l)\right) = 1.742652311\ldots.$$

COROLLARY 4. *If n is an integer greater than 2, then*

$$E(\mathbf{Z}_n^*) < \begin{cases} \omega(n) + \sigma, & n \equiv 1 \pmod 2 \\ \omega(n) + \sigma - 1, & n \equiv 2 \pmod 4 \\ \omega(n) + \sigma_2, & n \equiv 4 \pmod 8 \\ \omega(n) + \sigma_2 + 1, & n \equiv 0 \pmod 8. \end{cases}$$

While for specific numbers n the value of $E(\mathbf{Z}_n^*)$ is smaller, the constants in Corollary 4 are best possible when considering all numbers n. In particular, it follows from Dirichlet's theorem on primes in an arithmetic progression that for each fixed k, there are infinitely many primes p that are 1 more than a multiple of the product of the first k primes. If m is the product of k of these primes p and if k is large, then Corollary 4 is nearly best possible for $n = m, 2m, 4m$, and $8m$. The larger is the value of k, the closer Corollary 4 is to the truth for these numbers.

REMARKS. The argument at the start of the proof of the theorem is well known. In fact a more general result is known: a subset of a finite group G generates G if and only if the projection of the subset in $G/\Phi(G)$ generates $G/\Phi(G)$, where $\Phi(G)$ is the Frattini subgroup of G (the intersection of all maximal subgroups). Note too that the argument given for (2) works for any finite p-group G, since in this case, $G/\Phi(G)$ is also isomorphic to $\mathbf{F}_p^r$, as it is in the abelian case. We conclude that the entire proof goes through for any finite group G which is a product of p-groups for various primes p. That is, the theorem holds for all finite nilpotent groups. This observation should be compared with the discussion in [1].

We also remark that the methods of this paper may be used to compute higher moments for the random generation of finite abelian (or nilpotent) groups.

Finally I mention a recent paper [10] of Pak. Among many interesting results, some of which shed some light on the questions raised at the end of the Introduction of the present paper, he shows that for a finite nilpotent group G, the probability that $r(G) + 1$ random elements chosen from G actually generate G is $> 1/e$. It follows from (4) that this probability is $> c = 0.43575707677\ldots$, where c is the number defined in Corollary 2. Further, this inequality is false if c is replaced with any higher number. Pak also has a lower bound for the probability that G is generated by $r(G)+j$ random elements. Using (4) the greatest lower bound for this probability may be computed; it is $c\,\zeta(2)\zeta(3)\ldots\zeta(j)$ (cf. Corollary 2). Though it was not computed by Pak, using his inequalities one may similarly deduce as in the present paper that $e(G)$ is uniformly bounded over finite nilpotent groups, though the bound so obtained would be considerably larger than our bound σ.

ACKNOWLEDGEMENTS. I gratefully acknowledge some helpful conversations and correspondence with David Benson, John Dixon, Robert Guralnick, Hendrik Lenstra, Alexander Lubotzky, Péter Pálfy, Eric Schmutz, Amin Shokrollahi, Igor Shparlinski, Jacques Stern, Gang Yu, Alan Weiss, and Peter Winkler. In addition, the suggestions of the referee simplified the paper; I am grateful for the careful reading.

REFERENCES

[1] V. Acciaro, The probability of generating some common families of finite groups, *Util. Math.* **49** (1996), 243–254.

[2] J. P. Buhler, H. W. Lenstra, Jr., and C. Pomerance, Factoring integers with the number field sieve, in: *The development of the number field sieve*, A. K. Lenstra and H. W. Lenstra, Jr., eds., Lecture Notes in Math. **1554**, pp. 50–94, Springer-Verlag, Berlin, 1993.

[3] J. D. Dixon, The probability of generating the symmetric group, *Math. Z.* **110** (1969), 199–205.

[4] P. Erdős and G. Szekeres, Über die Anzahl der Abelschen Gruppen gegebener Ordnung und über ein verwandtes zahlentheoretisches Problem, *Acta Sci. Math. (Szeged)* **7** (1935), 95–102.

[5] A. Ivić, *The Riemann zeta-function*, Wiley, New York, 1985.

[6] W. M. Kantor and A. Lubotzky, The probability of generating a finite classical group, *Geom. Dedicata* **36** (1990), 67–87.

[7] S. Konyagin and C. Pomerance, On primes recognizable in deterministic polynomial time, in: *The mathematics of Paul Erdős*, vol. 1, R. L. Graham and J. Nešetřil, eds., pp. 176–198, Springer-Verlag, Berlin, 1997.

[8] H. W. Lenstra, Jr. and C. Pomerance, A rigorous time bound for factoring integers, *J. Amer. Math. Soc.* **5** (1992), 483–516.

[9] M. W. Liebeck and A. Shalev, The probability of generating a finite simple group, *Geom. Dedicata* **56** (1995), 103–113.

[10] I. Pak, On probability of generating a finite group, preprint, 1999.

[11] G. Poupard and J. Stern, Short proofs of knowledge of factoring, in: *Proc. PKC2000*, Lecture Notes in Comput. Sci. **1751**, pp. 147–166, Springer-Verlag, Berlin, 2000.

(Received: July 12, 2000)

Carl Pomerance
Fundamental Mathematics Research
Bell Labs – Lucent Technologies
Murray Hill, NJ 07974
USA
E-mail: carlp@research.bell-labs.com