The Factorial Function and Generalizations

Manjul Bhargava

1. INTRODUCTION. The factorial function hardly needs any introduction. Starting with its fundamental interpretation as the number of ways n people can sit in n chairs, to its occurrence in formulae for binomial coefficients, Stirling numbers, and countless other combinatorial objects, it is indeed nearly impossible to study any area of combinatorics without becoming intimately familiar with the factorial.

Perhaps it is due to this ubiquity in combinatorics that sometimes it is overlooked that the factorial also makes several important appearances in number theory! The purpose of this article is to take a closer look at some of these number-theoretic appearances, and thereby lead up to a series of generalizations of the factorial function, which recently have been applied to a variety of number-theoretic, ring-theoretic, and combinatorial problems.

The work described here began about four years ago as part of the author's thesis at Harvard University. The "generalized factorials" introduced there have since been used to give answers to some old questions; but more than that, they have given rise to several new questions that beg for answers. I hope that this expository account, together with several new results and observations, gives readers a sense of what these generalized factorials are all about, and at the same time, incites them to try their hand at some of the many very tempting questions that arise in the process!

2. THE FACTORIAL FUNCTION IN NUMBER THEORY? The most well-known instance of the factorial function arising in a number-theoretic context is probably the following divisibility result: *The product of any k consecutive integers must be divisible by k*!. Although admittedly a rather trivial statement, this result is more number-theoretically significant than it might first seem (indeed, we need it a bit later). The proof is of course quite simple; for we may restate this result as follows:

Theorem 1. *For any nonnegative integers k and ℓ, $(k+\ell)!$ is a multiple of $k!\,\ell!$.*

Theorem 1 is clearly equivalent to our original formulation, and moreover, its truth is clear combinatorially: the quotient $(k+\ell)!/k!\,\ell!$ is simply the binomial coefficient (and integer) $\binom{k+\ell}{k}$.

There are, however, many occurrences of the factorial function in number theory that are not quite so trivial. One beautiful such example, due to George Pólya, describes the close relationship between the factorial function and the possible sets of values taken by a polynomial.

Suppose we have a polynomial f with integer coefficients. The *fixed divisor* of f over the integers $\mathbb{Z}$, denoted by $d(\mathbb{Z}, f)$, is the greatest common divisor of all the elements in the image of f on $\mathbb{Z}$; that is,

$$d(\mathbb{Z}, f) = \gcd\{f(a) : a \in \mathbb{Z}\}.$$

For example, consider the polynomial $f(x) = x^5 + x$. If x is even, then $f(x)$ is even, and if x is odd, then again $f(x)$ is even. It follows that $d(\mathbb{Z}, f)$ must be a multiple of 2. On the other hand, we have $f(1) = 2$; hence $d(\mathbb{Z}, f)$ is exactly 2 in this case.

The question naturally arises: what are the possible values of $d(\mathbb{Z}, f)$? Can it be anything? Well, if we let $f(x) = 1000x^5 + 1000x$ (i.e., 1000 times the previous polynomial), then $d(\mathbb{Z}, f) = 2000$; that is, we can multiply an existing fixed divisor by anything we like simply by multiplying the polynomial by that amount. Therefore, we would like to answer this question for only those polynomials whose coefficients are relatively prime, i.e., for *primitive polynomials*.

In that case, our question has the following surprising answer, discovered by Pólya [**27**] in 1915:

Theorem 2. *Let f be a primitive polynomial of degree k, and let $d(\mathbb{Z}, f) = \gcd\{f(a) : a \in \mathbb{Z}\}$. Then $d(\mathbb{Z}, f)$ divides $k!$. (This is sharp!)*

By the phrase "this is sharp" we mean that not only is $k!$ an upper bound for the fixed divisor of a degree k polynomial, but $k!$ can actually be achieved for some primitive polynomial f; in fact, any factor of $k!$ can be achieved.

Now one may ask: what is $k!$ doing here? It's not immediately clear why the factorial function should appear in this result; yet it does. We explain this result from a more general viewpoint a little later.

But first, here is another pretty example of the factorial function arising in a number-theoretic context:

Theorem 3. *Let $a_0, a_1, \dots, a_n \in \mathbb{Z}$ be any $n + 1$ integers. Then the product of their pairwise differences*

$$\prod_{i<j} (a_i - a_j)$$

is a multiple of $0!\,1! \cdots n!$. (This is sharp!)

As before, "this is sharp" refers to the fact that the constant $0!1! \cdots n!$ in the statement of the theorem cannot be improved.

It is interesting to note that Theorem 3 originates in the representation theory of Lie algebras: the quotient $\prod_{i<j}(a_i - a_j)/0!1! \cdots n!$ is the dimension of a certain irreducible representation of $SU(n)$, and consequently must be an integer. This elegant result has been the subject of some recent articles (e.g., [**29**]), and was also once a problem posed on the Russian Mathematical Olympiad. Again, notice how the factorial function appears, and in this case how it does so numerous times.

Let us look at one more example of the factorial function for now—this one of a combinatorial nature. Recall that, for any given prime n, every function from $\mathbb{Z}/n\mathbb{Z}$ to itself can be represented by a polynomial. This is because when n is prime, $\mathbb{Z}/n\mathbb{Z}$ is a field, so one may carry out the usual Lagrange interpolation. When n is not prime, however, not every function is so representable; for when performing Lagrange interpolation, one often needs to divide, but this may not be possible in a nonfield. The question thus arises: how many functions from $\mathbb{Z}/n\mathbb{Z}$ to itself (equivalently, from $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$) are representable by a polynomial?

It so happens there is an exact formula for the number of such polynomial mappings, and it was discovered by Kempner [**18**] in the 1920's:

Theorem 4. *The number of polynomial functions from $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$ is given by*

$$\prod_{k=0}^{n-1} \frac{n}{\gcd(n, k!)}.$$

In particular, when n is prime, Theorem 4 tells us that there are n^n such functions; hence in this case every function from $\mathbb{Z}/n\mathbb{Z}$ to itself is polynomial, as was expected. Notice the appearance of the factorial function in the general formula.

3. THE MOTIVATING QUESTION.

To summarize, we have four—well, actually there are many more—but for now, we have four number-theoretic results in which the factorial function plays a very prominent role. But all these results involving factorials are heavily dependent on the fact that we are working in $\mathbb{Z}$—the entire set of rational integers. Indeed: in Theorem 2, we take the greatest common divisor of $f(a)$ over all a in $\mathbb{Z}$; in Theorem 3, we choose any $n + 1$ integers from $\mathbb{Z}$; in Theorem 4, we take polynomial mappings from $\mathbb{Z}$ to the integers modulo n; and so on.

What would happen if we were to change each of these occurrences of $\mathbb{Z}$ to something else? Perhaps to some subset S of $\mathbb{Z}$. Or to some other ring entirely. Or perhaps even to some subset of some other ring! Is there some other function—some generalized factorial function—that we could change each of the ordinary factorials to, so that Theorems 1–4 would still remain true?

It turns out there is such a "generalized factorial function" for *any* given subset S of $\mathbb{Z}$ that simultaneously makes Theorems 1–4 true when $\mathbb{Z}$ is replaced by S. In fact, the same holds true for any subset S of a Dedekind ring.

How can one construct these generalized factorials? Let us consider first the case when S is a subset of $\mathbb{Z}$.

4. A GAME CALLED p-ORDERING.

Let S be an arbitrary subset of $\mathbb{Z}$, and fix a prime p. A *p-ordering* of S is a sequence $\{a_i\}_{i=0}^{\infty}$ of elements of S that is formed as follows:

- Choose any element $a_0 \in S$;
- Choose an element $a_1 \in S$ that minimizes the highest power of p dividing $a_1 - a_0$;
- Choose an element $a_2 \in S$ that minimizes the highest power of p dividing $(a_2 - a_0)(a_2 - a_1)$;

and in general, at the kth step,

- Choose an element $a_k \in S$ that minimizes the highest power of p dividing $(a_k - a_0)(a_k - a_1) \cdots (a_k - a_{k-1})$.

Notice that a p-ordering of S is certainly not unique; indeed, the element a_0 is chosen arbitrarily, and at later steps there are frequently ties for which element achieves the desired minimum, and one may choose any one of these. In addition, each time one makes a choice for an a_k, it affects the choices one has in the future.

But once such a p-ordering $\{a_i\}_{i=0}^{\infty}$ has been constructed, one obtains a corresponding monotone increasing sequence $\{\nu_k(S, p)\}_{k=0}^{\infty}$ of powers of p, where the kth element $\nu_k(S, p)$ is the power of p minimized at the kth step of the

p-ordering process. More precisely, if we denote by $w_p(a)$ the highest power of p dividing a (e.g., $w_3(18) = 9$), then $\nu_k(S, p)$ is given by

$$\nu_k(S,p) = w_p((a_k - a_0) \cdots (a_k - a_{k-1})). \tag{1}$$

We refer to this sequence $\{\nu_k(S, p)\}$ as the *associated p-sequence* of S corresponding to the chosen p-ordering $\{a_i\}$ of S.

Now it would seem that since there are so many choices to be made when constructing a p-ordering, and since each choice so greatly affects all future choices, that the resulting sequence of minimal powers of p—the associated p-sequence—could be just about anything. But it turns out that:

Theorem 5. *The associated p-sequence of S is independent of the choice of p-ordering*!

Thus the associated p-sequence is intrinsic to S, dependent only on S, and we may speak of it without reference to any particular p-ordering.

Theorem 5 is not at all obvious a priori; however, by the end of the article, it should become very obvious indeed, and in many different ways!

5. THE PUNCHLINE. Let us move on to an example of a p-ordering. We start with the simplest possible case, namely the entire set of integers $\mathbb{Z}$. Then we have the following fact:

Proposition 6. *The natural ordering* $0, 1, 2, \ldots$ *of the nonnegative integers forms a p-ordering of* $\mathbb{Z}$ *for all primes p simultaneously.*

The proof is by induction: if $0, 1, 2 \ldots, k-1$ is a p-ordering for the first $k - 1$ steps, then at the kth step we need to pick a_k to minimize the highest power of p dividing

$$(a_k - 0)(a_k - 1) \cdots (a_k - (k-1)). \tag{2}$$

However, notice that (2) is the product of k consecutive integers; consequently it must be a multiple of $k!$. But $k!$ can actually be achieved, with the choice $a_k = k$; this value of a_k clearly minimizes the highest power of p dividing (2) for all primes p. So at the kth step we choose $a_k = k$, and the claim follows by induction. ■

Now since any p-ordering gives the same associated p-sequence, we are in the position to calculate the associated p-sequence $\nu_k(\mathbb{Z}, p)$ of $\mathbb{Z}$. We have

$$\begin{aligned}\nu_k(\mathbb{Z},p) &= w_p((a_k - a_0) \cdots (a_k - a_{k-1})) \\ &= w_p((k-0) \cdots (k-(k-1))) = w_p(k!).\end{aligned}$$

And aha! a factorial! In fact, if we take the expression $w_p(k!)$, and multiply over all primes p, then we get exactly $k!$. So we have a definition of the factorial function purely in terms of these invariants $\nu_k(\mathbb{Z}, p)$:

$$k! = \prod_p \nu_k(\mathbb{Z}, p).$$

But by Theorem 5, $\mathbb{Z}$ is not the only set that has these invariants ν_k—any set S has these invariants! This motivates the following definition:

Definition 7. Let S be any subset of $\mathbb{Z}$. Then the *factorial function* of S, denoted $k!_S$, is defined by

$$k!_S = \prod_p \nu_k(S, p). \tag{3}$$

In particular, we have $k!_{\mathbb{Z}} = k!$.

It is a fundamental lemma that the number of factors not equal to one in the product (3) is necessarily finite. Hence Definition 7 makes sense for all S and k.

This seems to be a very natural definition to make—and it turns out it really is the "correct" number-theoretic generalization of the factorial, in that even when $S \neq \mathbb{Z}$, $k!_S$ still shares many important number-theoretic properties with the usual factorial.

6. SOME OLD THEOREMS REVISITED.

For example, it is still true that (even for generalized factorials),

Theorem 8. *For any nonnegative integers k and ℓ, $(k + \ell)!_S$ is a multiple of $k!_S\, \ell!_S$.*

This implies, in particular, that we may associate a canonical set of binomial coefficients $\binom{n}{k}_S$ to any set $S \subseteq \mathbb{Z}$, by

$$\binom{n}{k}_S = \frac{n!_S}{k!_S(n-k)!_S}.$$

These generalized binomial coefficients surely must have many interesting properties of their own.

Theorem 8 is not quite as obvious as the result it generalizes. Indeed, as with Theorem 5, trying to prove this result directly from the definitions makes for a challenging (perhaps a bit frustrating?) exercise in combinatorics. In the next section, we give a very short proof of Theorem 8, based on our upcoming generalization of Pólya's Theorem 2.

Theorem 2 concerned the greatest common divisor $d(\mathbb{Z}, f)$ of the values of a primitive polynomial f on $\mathbb{Z}$. More generally, the *fixed divisor of f over S*, denoted by $d(S, f)$, is the greatest common divisor of the elements in the image of f on S. That is,

$$d(S,f) = \gcd\{f(a) : a \in S\}.$$

We may ask the same question about fixed divisors over S, namely: what are the possible values of $d(S, f)$ for primitive polynomials f?

Theorem 9. *Let f be a primitive polynomial of degree k, and let $d(S, f) = \gcd\{f(a) : a \in S\}$. Then $d(S, f)$ divides $k!_S$. (This is sharp!)*

As in Theorem 2, not only is $k!_S$ an upper bound on how large a fixed divisor of a primitive degree k polynomial can be on S, but $k!_S$ can actually be achieved (and as before, any factor of $k!_S$ can be achieved). Thus Theorem 9 extends Polya's result to a general setting.

The analogue of Theorem 3 can also be formulated in a similar manner. Suppose that we are required to choose our $n + 1$ integers not from $\mathbb{Z}$, but from within the set S. What then can we say about the product of their pairwise differences?

Theorem 10. *Let $a_0, a_1, \ldots, a_n \in S$ be any $n + 1$ integers. Then the product*

$$\prod_{i<j} (a_i - a_j)$$

is a multiple of $0!_S\, 1!_S \cdots n!_S$. (This is sharp!)

Again, the phrase "this is sharp" indicates that the constant $0!_S 1!_S \cdots n!_S$ cannot be improved.

As a simple example, suppose we take S to be the set of primes in $\mathbb{Z}$. Using the p-ordering algorithm, it is an easy matter to compute the first six factorials of S: $0!_S = 1$, $1!_S = 1$, $2!_S = 2$, $3!_S = 24$, $4!_S = 48$, and $5!_S = 5760$. Consequently, if $p_0, p_1, \ldots, p_5$ are any six primes, then Theorem 10 says that the product of their pairwise differences $\prod_{i<j}(p_i - p_j)$ is a multiple of 13,271,040. We may compare with the result of Theorem 3, which by itself shows only that it is a multiple of 34,560.

Finally, we consider the analogue of Kempner's result, Theorem 4. Just as before, when n is prime, any function from a subset S of $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$ can be represented by a polynomial. When n is not prime, though, this is no longer the case. How many functions from S to $\mathbb{Z}/n\mathbb{Z}$ are polynomial?

Theorem 11. *The number of polynomial functions from S to $\mathbb{Z}/n\mathbb{Z}$ is given by*

$$\prod_{k=0}^{n-1} \frac{n}{\gcd(n, k!_S)}.$$

As the reader can tell, creating Theorems 8–11 was quite easy: it was done simply by changing all the previous occurrences of $\mathbb{Z}$'s in Theorems 1–4 to S's, and all the previous !'s to $!_S$'s. And remarkably, all the theorems remain true!

The same happens with many other theorems as well—we provide some further examples in Sections 11 and 13. But first, let us take a detour and indicate why all the aforementioned results are true. (If desired, the reader may skip the next section for the time being without loss of continuity.)

7. PROOFS OF THEOREMS 5 AND 8–11.

The simplest proofs of Theorem 5 and Theorems 8–11 are probably via the following observations. Often, when writing polynomials, it is more convenient to use the "falling factorial" basis

$$x^{(n)} = x(x-1)\cdots(x-n+1), \quad n \geq 0,$$

rather than the more familiar basis $\{x^n : n \geq 0\}$. Indeed, much of the difference calculus is based on the important properties of these polynomials $x^{(n)}$.

It turns out that we may define an analogue of the falling factorial for any set $S \subseteq \mathbb{Z}$; namely, having fixed a p-ordering $\{a_i\}$ of S, define $x^{(n)_{S,p}}$ by

$$x^{(n)_{S,p}} = (x - a_0)(x - a_1)\cdots(x - a_{n-1}).$$

In the case $S = \mathbb{Z}$ with p-ordering $0, 1, 2, \ldots$, these polynomials coincide with the usual falling factorials $x^{(n)}$.

The generalized falling factorials $x^{(n)_{S,p}}$ can be used to develop a difference calculus for S. Although we do not need here the full details of this theory, the following result is worth mentioning:

Lemma 12. *A polynomial f over the integers, written in the form*

$$f(x) = \sum_{i=0}^{k} c_i x^{(i)_{S,p}} = \sum_{i=0}^{k} c_i (x - a_0)(x - a_1)\cdots(x - a_{i-1}), \tag{4}$$

vanishes on S modulo p^e if and only if $c_i x^{(i)_{S,p}}$ does for each $0 \leq i \leq k$.

Proof: Suppose f vanishes on S (mod p^e), but some term on the right side of (4) does not. Then let j be the smallest index for which $c_j x^{(j)_{S,p}}$ does not vanish on S (mod p^e). Setting $x = a_j$ in (4), we find that all terms on the right side with $i > j$ vanish identically, whereas the minimality of j guarantees that all terms with $i < j$ vanish (mod p^e). It follows that $c_j a_j^{(j)_{S,p}}$ also vanishes (mod p^e), and consequently $c_j x^{(j)_{S,p}}$ vanishes on all of S (mod p^e), since $\{a_i\}$ is a p-ordering. This contradiction proves the lemma. ■

We may now prove Theorems 8–11 in no time at all. We begin with our extension of Pólya's theorem, Theorem 9.

Proof of Theorem 9: For a fixed prime p, and a choice of p-ordering $\{a_i\}$ of S, write f in the form

$$f = \sum_{i=0}^{k} c_i x^{(i)_{S,p}} = \sum_{i=0}^{k} c_i (x - a_0)(x - a_1) \cdots (x - a_{i-1}). \tag{5}$$

Since f is primitive, there is a choice of j $(0 \leq j \leq k)$ such that c_j is not a multiple of p. Now by definition f vanishes on S modulo $w_p(d(S,f))$; hence Lemma 12 ensures that $c_j x^{(j)_{S,p}}$ does also. Moreover, since c_j is relatively prime to p, it follows that $x^{(j)_{S,p}}$ vanishes on S modulo $w_p(d(S,f))$. In particular, $w_p(d(S,f))$ divides

$$w_p\left(a_j^{(j)_{S,p}}\right) = w_p\left((a_j - a_0)(a_j - a_1) \cdots (a_j - a_{j-1})\right) = w_p(j!_S);$$

hence $w_p(d(S,f))$ divides $w_p(k!_S)$, since $j!_S$ divides $k!_S$. Multiplying over all p, we see that $d(S,f)$ divides $k!_S$, as desired.

To see that $k!_S$ (and any factor thereof) can actually be achieved, we construct "global falling factorial" polynomials $B_{k,S}$ by setting

$$B_{k,S}(x) = (x - a_{0,k})(x - a_{1,k}) \cdots (x - a_{k-1,k}), \tag{6}$$

where $\{a_{i,k}\}_{i=0}^{\infty}$ is a sequence in $\mathbb{Z}$ that, for each prime p dividing $k!_S$, is termwise congruent modulo $\nu_k(S,p)$ to some p-ordering of S. Then it is clear that $d(S, B_{k,S}) = k!_S$. Furthermore, if r is any factor of $k!_S$, then $d(S, B_{k,S} + r) = r$; hence any factor of $k!_S$ can be obtained as a fixed divisor of some primitive polynomial. ■

Theorem 9 turns out to be a very powerful tool in understanding generalized factorials. For example, it can be used to give a wonderfully quick proof of Theorem 8:

Proof of Theorem 8: By Theorem 9, there exist primitive polynomials f_k (e.g., $B_{k,S}$) and f_{n-k} (e.g., $B_{n-k,S}$) having degrees k and $n-k$ respectively, such that $d(S, f_k) = k!_S$ and $d(S, f_{n-k}) = (n-k)!_S$. By multiplication, we obtain a primitive polynomial $f = f_k f_{n-k}$ of degree n such that $k!_S(n-k)!_S$ divides $d(S,f)$. But by Theorem 9 again, we know $d(S,f)$ must divide $n!_S$. Hence $k!_S(n-k)!_S$ divides $n!_S$, as desired. ■

Another important property of generalized factorials is given in the following lemma. Like Theorem 8, it also is not quite as innocent as it first looks, though Theorem 9 again provides the key to an easy proof.

Lemma 13. *Let $T \subseteq S$. Then $k!_S$ divides $k!_T$ for every $k \geq 0$.*

Proof: For any polynomial f, clearly $d(S,f)$ divides $d(T,f)$. Thus, in particular, $d(S, B_{k,S}) = k!_S$ divides $d(T, B_{k,S})$, and by Theorem 9, the latter must divide $k!_T$. It follows that $k!_S$ divides $k!_T$. ■

Lemma 13 may be used to provide a quick proof of Theorem 10.

Proof of Theorem 10: For a fixed prime p, assume that $a_0, a_1, \ldots, a_n$ are the first $n+1$ elements of a p-ordering of the set $T = \{a_0, a_1, \ldots, a_n\}$. Then since for each $0 \leq k \leq n$,

$$\nu_k(T,p) = w_p((a_k - a_0)(a_k - a_1)\cdots(a_k - a_{k-1})),$$

we find, upon taking the product over all k and then over all p, that

$$0!_T 1!_T \cdots n!_T = \pm \prod_{i<j}(a_j - a_i).$$

Now by Lemma 13, we know $k!_S$ divides $k!_T$. Therefore

$$0!_S 1!_S \cdots n!_S \Big| \prod_{i<j}(a_i - a_j),$$

proving the first assertion of the theorem.

As for the second assertion, observe that if T consists of the first $n+1$ elements of a p-ordering of S, then

$$w_p\left(\prod_{i<j}(a_i - a_j)\right) = \nu_0(S,p)\nu_1(S,p)\cdots\nu_n(S,p) = w_p(0!_S 1!_S \cdots n!_S);$$

hence $0!_S 1!_S \cdots n!_S$ cannot be replaced by a larger constant in the statement of the theorem. ■

For the proof of Theorem 11, we need the following refinement of Lemma 12:

Lemma 14. *A polynomial f of degree d, written in the form*

$$f(x) = \sum_{k=0}^{d} x^{(k)_{S,p}} = \sum_{k=0}^{d} b_k(x - a_0)(x - a_1)\cdots(x - a_{k-1}),$$

vanishes on S modulo p^e if and only if b_k is a multiple of $\frac{p^e}{\gcd(p^e, k!_S)}$ for each $0 \leq k \leq d$.

Proof: By Lemma 12, $f(x)$ vanishes on S modulo p^e if and only if $b_k x^{(k)_{S,p}}$ does for each $0 \leq k \leq d$. Now by construction of $x^{(k)_{S,p}}$, we have $w_p(d(S, x^{(k)_{S,p}})) = \nu_k(S,p)$; hence $b_k x^{(k)_{S,p}}$ vanishes on S modulo p^e if and only if b_k is a multiple of $p^e/\gcd(p^e, k!_S)$. This is the desired conclusion. ■

Proof of Theorem 11: By the Chinese Remainder Theorem, specifying a polynomial mapping on S (modulo n) is equivalent to specifying the mapping modulo each prime power dividing n. Now it is easily seen that the formula of Theorem 11 is multiplicative; hence it suffices to verify Theorem 11 when $n = p^e$ is a prime power.

Let $\{a_i\}$ be a p-ordering of S. Then we claim that *any polynomial mapping* $f{:}S \to \mathbb{Z}/p^e\mathbb{Z}$ *can be expressed uniquely in the form*

$$f(x) = \sum_{k=0}^{\infty} c_k(x - a_0)(x - a_1)\cdots(x - a_{k-1}), \tag{7}$$

where $0 \le c_k < p^e/\gcd(p^e, k!_S)$ *for each* $k \ge 0$. Indeed, by Lemma 14, changing one of the coefficients c_k by a multiple of $p^e/\gcd(p^e, k!_S)$ in (7) does not change the function f. That is to say, the c_k are determined only modulo $p^e/\gcd(p^e, k!_S)$, so we may choose them to lie in the range $0 \le c_k < p^e/\gcd(p^e, k!_S)$.

We now have a unique representative for each polynomial mapping from S to $\mathbb{Z}/p^e\mathbb{Z}$. Observing that there are $p^e/\gcd(p^e, k!_S)$ choices of c_k for each $k \ge 0$ yields the desired formula. ■

Any of Theorems 9–11 may now be used to give a proof of Theorem 5.

Proof of Theorem 5: Since none of Theorems 9–11 mention p-orderings, but they do involve (and in fact define) the generalized factorials, the definition of factorials given in Section 4 could not possibly depend on any choices of p-ordering! ■

Probably a more direct, conceptual way of seeing the truth of Theorem 5 is the following. For a positive integer d, and a large positive integer e such that $p^e > \nu_d(S, p)$, consider as an additive group the set G_d of all polynomials in $(\mathbb{Z}/p^e\mathbb{Z})[x]$ that vanish on S modulo p^e and have degree at most d. Then Lemma 12 implies that as an abelian group, G is isomorphic to

$$\bigoplus_{k=0}^{d} \mathbb{Z}/\nu_k(S, p)\mathbb{Z}.$$

Thus the numbers $\nu_k(S, p)$ (for $0 \le k \le d$) form the structure coefficients of this abelian group G_d; moreover, by the structure theorem for finitely generated abelian groups, these constants depend only on G_d itself, implying Theorem 5.

8. A MORE GENERAL FRAMEWORK: DEDEKIND RINGS. Much of what we have said holds for a more general class of rings, which we may call *Dedekind rings*. A Dedekind ring is any Noetherian, locally principal ring in which all nonzero primes are maximal. This class of rings includes, for example, Dedekind domains, such as the ring of integers in an algebraic number field or a polynomial ring over a finite field. It also includes any quotients of such rings, such as $\mathbb{Z}/n\mathbb{Z}$, Galois rings, and all finite principal ideal rings.

Thus for any subset S of a Dedekind ring R, there is a corresponding sequence of factorials. However, when working in R, one constructs P-orderings using prime ideals P of R rather than prime elements p of $\mathbb{Z}$. Consequently, the factorials of a set $S \subseteq R$ in general must be considered ideals in R.

For rings R that have a canonical generator for each ideal (e.g., $\mathbb{Z}$), the factorials may also then be thought of as elements of R.

9. SOME EXAMPLES OF GENERALIZED FACTORIALS. In this section, we take a look at some natural examples of generalized factorials. We've already seen one such:

Example 15. Let $S = \mathbb{Z}$. Then $k!_{\mathbb{Z}} = k!$.

In Example 15, there is a sequence in S that is a p-ordering of S for all primes p simultaneously (namely $0, 1, 2, \dots$). Although such an event is rare for general sets S, there are several important sets for which it does occur. Moreover, the factorials in such cases become especially easy to compute. We state this more precisely in the following lemma (whose proof follows trivially from the definitions).

Lemma 16. *Suppose $\{a_i\}$ is a p-ordering of S for all primes p simultaneously. Then*

$$k!_S = |(a_k - a_0)(a_k - a_1) \cdots (a_k - a_{k-1})|.$$

Lemma 16 is used in our next three examples.

Example 17. Let S be the set of even integers $2\mathbb{Z}$ in $\mathbb{Z}$. Then by the same argument as in Proposition 6, we find that the natural ordering $0, 2, 4, 6, \dots$ of $2\mathbb{Z}_{\geq 0}$ forms a p-ordering of $2\mathbb{Z}$ for all primes p. Hence, by Lemma 16, $k!_{2\mathbb{Z}} = (2k - 0)(2k - 2) \cdots (2k - (2k - 2)) = 2^k k!$. In a similar manner, we find that the set $a\mathbb{Z} + b$ of all integers that are b modulo a has factorials given by $k!_{a\mathbb{Z}+b} = a^k k!$.

Example 18. Let S be the set of powers of 2 in $\mathbb{Z}$. Then it is easy to verify that $1, 2, 4, 8, \dots$ forms a p-ordering of S for all p; hence $k!_S = (2^k - 1)(2^k - 2) \cdots (2^k - 2^{k-1})$. More generally, suppose we take any geometric progression S in $\mathbb{Z}$ with common ratio q and first term a. Then $k!_S = a^k(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})$.

Example 19. Let S be the set of square numbers in $\mathbb{Z}$. Then one can show by analysis of quadratic residues modulo p^n for each p that $0, 1, 4, 9, \dots$ forms a p-ordering of S for all primes p. It follows that

$$k!_S = (k^2 - 0)(k^2 - 1) \cdots \left(k^2 - (k - 1)^2\right) = \frac{(2k)!}{2}.$$

Theorem 10 applied to Example 19 proves the following result, which also originates in the representation theory of Lie algebras:

Theorem 20. *Let $a_0, a_1, \dots, a_n \in \mathbb{Z}$ be any $n + 1$ integers. Then the product of the pairwise differences of their squares*

$$\prod_{i<j} \left(a_i^2 - a_j^2\right)$$

is a multiple of $\frac{0!\,2! \cdots (2n)!}{2^{n+1}}$. (This is sharp!)

As we mentioned, Theorem 20 arises in representation theory: the quotient $2^{n+1}\prod_{i<j}(a_i^2 - a_j^2)/0!\,2! \cdots (2n)!$ is the dimension of a certain irreducible representation of $Sp(n)$.

Finally, we give one natural example of a subset S of $\mathbb{Z}$ that does not possess any simultaneous p-ordering; consequently, the formula for its factorials is a little more involved.

Example 21. Let S be the set of primes in $\mathbb{Z}$. Then for a fixed prime p, one can show that a p-ordering of S is given by a sequence $\{a_i\}$ having the following property: for each $e \geq 0$, the set $\{a_0, \dots, a_{p^{e-1}(p-1)}\}$ equals $(\mathbb{Z}/p^e\mathbb{Z})^* \cup \{p\}$ when considered modulo p^e. (Such a sequence $\{a_i\}$ is guaranteed to exist for every p by Dirichlet's Theorem.) The factorials of S are therefore given by

$$k!_S = \prod_p p^{\left\lfloor \frac{k-1}{p-1} \right\rfloor + \left\lfloor \frac{k-1}{p(p-1)} \right\rfloor + \left\lfloor \frac{k-1}{p^2(p-1)} \right\rfloor + \cdots}.$$

The factorials of the set of primes seem to be strangely connected with the Bernoulli numbers. Precisely, it appears that $k!_S$ is given simply by $2^{\lfloor \frac{n}{2} \rfloor}$ times the product of the denominators of the first $\left\lceil \frac{n}{2} \right\rceil$ Bernoulli numbers. This assertion may be verified using the von Staudt Theorem **[24]**; but is there a deeper explanation of this rather striking connection?

10. SOME SPECIAL CASES.

There are many previous generalizations of factorial that can be obtained as natural special cases of the definitions we have made here.

Example 18 is reminiscent of the well-known q-factorials that arise in enumerative combinatorics. In fact, one can obtain the abstract q-factorials directly as follows: let S be the set $\{(q^k - 1)/(q - 1)\colon k \in \mathbb{N}\}$ in the ring $\mathbb{C}[q, q^{-1}]$. (We invert q in the ring to kill the prime q.) Then we find as in Example 18 that

$$k!_S = (q-1)^{-k}(q^k - 1)(q^{k-1} - 1) \cdots (q - 1),$$

which is indeed just the kth q-factorial.

Another natural ring on which to try out the factorial construction is $\mathbb{F}_q[t]$, the ring of polynomials over the finite field of q elements. For $S = R = \mathbb{F}_q[t]$, a t-ordering of S may be constructed as follows: let $a_0, a_1, \ldots, a_{q-1}$ be the elements of $\mathbb{F}_q$ (with $a_0 = 0$), and define a_k in general by

$$a_k = a_{c_0} + a_{c_1} t + \cdots + a_{c_h} t^h,$$

where $\sum_{i=0}^h c_i q^i$ is the base q expansion of k. One then easily verifies that this gives a P-ordering of $\mathbb{F}_q[t]$ not only for $P = (t)$, but for all primes $P \subset \mathbb{F}_q[t]$. It follows that

$$\begin{aligned} k!_{\mathbb{F}_q[t]} &= (a_k - a_0) \cdots (a_k - a_{k-1}) \\ &= \left(t^{q^h} - t\right)^{c_h} \left(t^{q^{h-1}} - t\right)^{c_{h-1} + c_h q} \cdots \left(t^q - t\right)^{c_1 + \cdots + c_h q^{h-1}} \end{aligned}$$

where again $\sum_{i=0}^h c_i q^i$ denotes the base q expansion of k. We have arrived at the well-known "Carlitz factorials." In 1938, Carlitz **[9]** used these factorials to construct the Carlitz module, the first example of a Drinfeld module **[15]**.

The generalized factorials of Pólya **[28]**, Ostrowski **[26]**, and Gunji-McQuillan **[16]** can also be obtained from our construction, upon setting $S = R$ to be the ring of integers in a number field. In addition, setting $S = R$ to be the ring of integers in a function field over a finite field gives rise to what are known as the Γ-ideals of Goss **[13]**; they have been used by Goss as extensions of the Carlitz factorial to other function fields.

That all these classical factorials can be obtained as natural special cases of the factorials we have defined here seems to be further evidence that we have arrived at a "correct" notion of generalized factorial.

11. BASES FOR INTEGER-VALUED POLYNOMIALS.

When does a polynomial take integer values on the integers? The polynomial need not have integer coefficients for this to occur, for observe that the polynomial $f(x) = x(x-1)/2$, which has noninteger coefficients, still maps the integers to the integers. In fact, all the binomial polynomials $\binom{x}{k} = x(x-1)\cdots(x-k+1)/k!$ take integer values on the integers.

Can one classify all polynomials with this property? In 1915, Pólya gave an elegant answer to this question, by proving the following elementary but classical result:

Theorem 22 (Pólya [27]). *A polynomial is integer-valued on $\mathbb{Z}$ if and only if it can be written as a $\mathbb{Z}$-linear combination of the polynomials*

$$\binom{x}{k} = \frac{x(x-1)\cdots(x-k+1)}{k!},$$

$k = 0, 1, 2, \ldots.$

Thus the binomial polynomials, and all polynomials that can be obtained from them via addition and subtraction, are all the polynomials that are integer-valued on $\mathbb{Z}$. This result has had numerous applications, in algebraic geometry (e.g., in the theory of Hilbert polynomials), representation theory (e.g., in the theory of Chevalley groups), number theory (e.g., in the theory of Mahler expansions), as well as in combinatorics.

Subsequent to proving Theorem 22, Pólya wondered as to what generality this result could be extended. That is, for a subset S of a Dedekind domain R, when does there exist a similar *regular basis* (an R-basis consisting of one polynomial of each degree) for the set of R-valued polynomials on S? Pólya [**28**] answered this question when $S = R$ is the ring of integers in a quadratic number field (i.e., he characterized quadratic fields possessing such a regular basis, and gave an explicit construction of such a basis whenever it existed). Ostrowski [**26**] shortly thereafter extended Pólya's work to the case when $S = R$ is the ring of integers in a general number field. In the years since 1919, analogous results have been proved for various other possibilities of S and R (e.g., [**7**], [**11**], [**12**]), though an answer for general S and R was never obtained.

From our point of view, though, the answer to Pólya's question is easily guessed. Namely, we expect the factorials in the denominators of $\binom{x}{k}$ in Theorem 22 to be replaced by generalized factorials, and the numerators to be replaced by the generalized "falling factorials" $B_{k,S}$ of Section 7. We thereby obtain the following result:

Theorem 23. *A polynomial is integer-valued on a subset S of $\mathbb{Z}$ if and only if it can be written as a $\mathbb{Z}$-linear combination of the polynomials*

$$\frac{B_{k,S}}{k!_S} = \frac{(x-a_{0,k})(x-a_{1,k})\cdots(x-a_{k-1,k})}{k!_S},$$

$k = 0, 1, 2, \ldots,$ *where the $B_{k,S}$ are the polynomials defined in* (6).

For a subset S of a general Dedekind domain R, the answer is just slightly more complicated, but again not hard to guess. When constructing our basis for the set of polynomials R-valued on S, we wish to divide our polynomials $B_{k,S}$ by the generalized factorials $k!_S$; but these factorials, being ideals in general, may not have a single generator that we can divide by! The condition, therefore, for a regular basis to exist is that every ideal $k!_S$ be principal.

Theorem 24. *The set of polynomials that are R-valued on a subset S of a Dedekind domain R has a regular basis if and only if $k!_S$ is a principal ideal for all $k \geq 0$. If this is the case, then a regular basis may be given as in Theorem* 23.

Thus this fundamental problem about integer-valued polynomials, first put forth by Pólya in 1919, is now resolved.

12. EXTENSION TO SEVERAL VARIABLES. Much of the formalism developed in the previous sections for studying polynomials in one variable can be extended to the case of several variables. Indeed, the problem is equivalent to understanding what the correct definition of "factorial" is for subsets S of $\mathbb{Z}^n$ when $n > 1$. A key observation in accomplishing this is suggested by Theorem 10, which states that choosing a_k to minimize the product (1) is equivalent to minimizing the highest power of p dividing the Vandermonde determinant

$$\begin{vmatrix} 1 & a_0 & a_0^2 & \cdots & a_0^k \\ 1 & a_1 & a_1^2 & \cdots & a_1^k \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_k & a_k^2 & \cdots & a_k^k \end{vmatrix} = \prod_{i<j} (a_i - a_j). \tag{8}$$

In fact, we showed in [3] that $\nu_0(S, p), \nu_1(S, p), \ldots, \nu_k(S, p)$ give the p-parts of the elementary divisors of the Vandermonde matrix (8). This motivates the following more general definitions:

Definition 25. Let S be a subset of $\mathbb{Z}^n$ (or of R^n, where R is any Dedekind ring). Then for a fixed ordering $M_0, M_1, \ldots$ of the monomials of $\mathbb{Z}[x_1, \ldots, x_n]$, a *p-ordering* of S is a sequence $\mathbf{a}_0, \mathbf{a}_1, \ldots$ of elements in S inductively chosen to minimize the highest power of p dividing the determinant

$$V(\mathbf{a}_0, \mathbf{a}_1, \ldots, \mathbf{a}_k) = \begin{vmatrix} M_0(\mathbf{a}_0) & M_1(\mathbf{a}_0) & M_2(\mathbf{a}_0) & \cdots & M_k(\mathbf{a}_0) \\ M_0(\mathbf{a}_1) & M_1(\mathbf{a}_1) & M_2(\mathbf{a}_1) & \cdots & M_k(\mathbf{a}_1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ M_0(\mathbf{a}_k) & M_1(\mathbf{a}_k) & M_2(\mathbf{a}_k) & \cdots & M_k(\mathbf{a}_k) \end{vmatrix}.$$

The *associated p-sequence* of S is then given by

$$\nu_k(S, p) = w_p\left(\frac{V(\mathbf{a}_0, \mathbf{a}_1, \ldots, \mathbf{a}_n)}{V(\mathbf{a}_0, \mathbf{a}_1, \ldots, \mathbf{a}_{n-1})} \right),$$

and the *generalized factorial* $k!_S$ is

$$k!_S = \prod_p \nu_k(S, p).$$

One may verify that Definition 25, for $n = 1$ (and the usual monomial ordering $1, x, x^2, \ldots$), coincides with the notions of p-ordering, associated p-sequence, and generalized factorial given in Sections 4 and 5. Moreover, all the analogues of Theorems 5, 9–11, 23, and 24 can now be proved when S is a subset of $\mathbb{Z}^n$ (or R^n), using essentially the same techniques.

13. FURTHER APPLICATIONS. The concepts of p-ordering and generalized factorial have had some important applications to interpolation problems. We hinted at one of these problems earlier—the polynomial interpolation problem in

$\mathbb{Z}/n\mathbb{Z}$. As we have mentioned, traditional methods for performing polynomial interpolation do not work in general for subsets of $\mathbb{Z}/n\mathbb{Z}$, because these methods frequently require division operations that may not make sense in a nonfield such as $\mathbb{Z}/n\mathbb{Z}$.

But as we noted in the proof of Theorem 11, it suffices to understand the interpolation problem for $\mathbb{Z}/n\mathbb{Z}$ when $n = p^e$ is a power of a prime. In this case, it turns out that if one interpolates along a p-ordering in a certain way, then all such division-related problems can be completely avoided, and one obtains a general interpolation formula for functions on subsets of $\mathbb{Z}/n\mathbb{Z}$ (or for subsets of any finite principal ideal ring). Details may be found in [**2**].

Another area in which the ideas of this article have proved to be very useful is *p-adic interpolation.* A classical theorem of Mahler [**21**] states that that every continuous function f from the p-adic ring $\mathbb{Z}_p$ to its quotient field $\mathbb{Q}_p$ (or to any finite extension thereof) can be expressed uniquely in the form

$$f(x) = \sum_{n=0}^{\infty} c_n \binom{x}{n},$$

where the sequence c_n tends to 0 as $n \to \infty$. Do analogous series exist for other compact subsets of $\mathbb{Q}_p$, or for subsets of local fields other than $\mathbb{Q}_p$? There have been several partial results in this direction, such as the work of Amice [**1**], who provided answers for certain "well-distributed" sets S.

But as with Theorem 22, from our point of view it is easy to guess what the general answer should be:

Theorem 26. *Let S be any compact subset of a local field K. Then every continuous map $f : S \to K$ can be expressed uniquely in the form*

$$f(x) = \sum_{n=0}^{\infty} c_n \frac{B_{n,S}(x)}{n!_S}, \tag{9}$$

where the sequence c_n tends to 0 as $n \to \infty$.

In joint work with K. Kedlaya [**5**], Theorem 26 was proved, thus solving this p-adic interpolation problem for any compact subset of a local field. Moreover, by using the ideas described in Section 12, Theorem 26 has also recently been extended to the case of several variables, and in fact to arbitrary algebraic varieties over a discrete valuation domain; details may be found in [**6**]. For a simple treatment of locally analytic functions from this point of view, which fully extends Amice's work to general compact subsets S, see [**4**].

Also worth noting in this regard is the recent work of Maulik [**22**], who has used the ideas of p-ordering and generalized factorials to count the number of subsets of $\mathbb{Z}/n\mathbb{Z}$ that form the set of roots of some polynomial over $\mathbb{Z}/n\mathbb{Z}$.

14. SOME QUESTIONS.

In the previous sections we have seen some excellent evidence that the generalized factorials defined here are the "right" number-theoretic generalizations of the factorial function to arbitrary subsets S of $\mathbb{Z}$. Are they in any sense the correct combinatorial generalization?

Question 27. *For a subset $S \subset \mathbb{Z}$, is there a natural combinatorial interpretation of $k!_S$?*

What makes an affirmative answer to Question 1 seem probable is that the generalized binomial coefficients

$$\binom{n}{k}_S = \frac{n!_S}{k!_S(n-k)!_S}$$

are always integral. Besides our tricky proof of this fact in Section 7, what is a good reason for this to be true?

Question 28. *For a subset $S \subset \mathbb{Z}$, is there a natural combinatorial interpretation for $\binom{n}{k}_S$?*

As is well-known, the factorial function has a natural extension to a continuous function on the positive reals, called the gamma function; it may be defined by

$$\Gamma(x+1) = \int_0^\infty e^{-t}t^x\,dt.$$

In addition, the gamma function may be meromorphically continued to the entire complex plane. Might there exist, for each subset S of $\mathbb{Z}$, a natural and meromorphic generalized gamma function $\Gamma_S(x)$ defined on the real/complex numbers such that $\Gamma_S(n+1) = n!_S$ for all $n \geq 0$, and $\Gamma_{\mathbb{Z}}(x) = \Gamma(x)$?

The factorial function also has similar "extensions" to the p-adic fields $\mathbb{Q}_p$; the most successful such interpolations are probably the well-known p-adic gamma functions $\Gamma_p(x)$ of Morita **[25]**. Again, it is natural to ask whether analogous p-adic interpolations $\Gamma_{S,p}$ might exist for the generalized factorials associated to other sets S.

Question 29. *For general subsets S of $\mathbb{Z}$ (or of other Dedekind domains), are there natural complex (respectively, p-adic) analytic interpolations of $k!_S$ to generalized gamma functions Γ_S (respectively, $\Gamma_{S,p}$)?*

Positive answers to Question 29 have been given for many of the special cases of generalized factorials listed in Section 10. For q-factorials, a natural complex analytic gamma function interpolating them has been given by Jackson **[17]**, and natural p-adic extensions have been carried out by Koblitz **[19]**. P-adic extensions of the Carlitz factorials $k!_{\mathbb{F}_q[t]}$ were discovered by Goss **[14]**. For general function fields, different factorials were defined and interpolated by Thakur **[30]**.

But as we've just seen, the special cases of our factorials for which P-adic gamma functions have been found all correspond to sets that possess simultaneous P-orderings. In fact, Dinesh Thakur has suggested the possibility that natural gamma functions interpolating these generalized factorials might exist only for sets S that have such simultaneous P-orderings. Thus the following question, interesting in its own right, may also be relevant in answering Question 29.

Question 30. *Which subsets S of $\mathbb{Z}$ (or of a Dedekind ring R) have simultaneous p-orderings for all primes p?*

An answer to Question 30 is not known even when $S = R$, where R is the ring of integers in a number field or function field. Even partial answers in these cases would be of much interest.

These were some of the questions I posed to the audience in San Diego, while giving the 1997 AMS-MAA address on which this article is based. But my audience had many other excellent questions! Here are a few of them:

Question 31. *What are analogues of Stirling's formula for generalized factorials?*

Question 32. *What is the "binomial theorem" for generalized binomial coefficients?*

Question 33. *What is the S-analogue of the exponential function*

$$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!},$$

and what properties does it have?

As is evident, there is much left to understand! We have considered here just a few of the many natural questions one may ask about generalized factorials. We expect that many of these questions have very nice answers, and hope that the examples and results included in this article will help in resolving some of these questions in the near future!

ACKNOWLEDGMENTS. I am thankful to Timothy Chow, Keith Conrad, Persi Diaconis, Joseph Gallian, Danny Goldstein, Kiran Kedlaya, Barry Mazur, Lenny Ng, Gian-Carlo Rota, Richard Stanley, and Dinesh Thakur for their encouragement and valuable conversations about generalized factorials over the past few years. Some parts of this work were done during the 1995 Summer Research Program at the University of Minnesota, Duluth, directed by Joseph Gallian and sponsored by the National Science Foundation (grant DMS-9225045) and the National Security Agency (grant number MDA 904-91-H-0036); other parts were supported by a Hertz fellowship.

REFERENCES

1. Y. Amice, Interpolation p-adique, *Bull. Soc. Math. France* **92** (1964) 117–180.
2. M. Bhargava, P-orderings and polynomial functions on arbitrary subsets of Dedekind rings, *J. reine angew. Math.* **490** (1997) 101–127.
3. M. Bhargava, Generalized factorials and fixed divisors over subsets of a Dedekind domain, *J. Number Theory* **72** (1998) 67–75.
4. M. Bhargava, Integer-valued polynomials and p-adic locally analytic functions, preprint.
5. M. Bhargava and K. S. Kedlaya, Continuous functions on compact subsets of local fields, *Acta Arith.* **91** (1999) 191–198.
6. M. Bhargava and K. S. Kedlaya, An analogue of Mahler's theorem for algebraic varieties over a discrete valuation domain, in preparation.
7. P.-J. Cahen, Polynômes à valeurs entières, *Canad. J. Math.* **24** (1972) 747–754.
8. P.-J. Cahen and J.-L. Chabert, *Integer-valued polynomials*, Mathematical Surveys and Monographs, 48, American Mathematical Society, Providence, RI, 1997.
9. L. Carlitz, A class of polynomials, *Trans. Amer. Math. Soc.* **43** (1938) 167–182.
10. L. Carlitz, Functions and polynomials (mod p^n), *Acta Arith.* **9** (1964) 67–78.
11. J.-L. Chabert, S. T. Chapman, and W. W. Smith, A basis for the ring of polynomials integer-valued on prime numbers, in *Factorization in integral domains*, Lecture Notes in Pure and Appl. Math., 189, Dekker, New York, 1997, pp. 271–284.
12. R. Gilmer, Sets that determine integer-valued polynomials, *J. Number Theory* **33** (1989) 95–100.
13. D. Goss, The Γ-ideal and special zeta-values, *Duke Math. J.* **47** (1980) 345–364.
14. D. Goss, The Γ-function in the arithmetic of function fields, *Duke Math. J.* **56** (1988) 163–191.
15. D. Goss, *Basic structures of function field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), 35, Springer-Verlag, Berlin, 1996.
16. H. Gunji and D. L. McQuillan, On a class of ideals in an algebraic number field, *J. Number Theory* **2** (1970) 207–222.
17. F. H. Jackson, On q-definite integrals, *Quart. J. Pure and Appl. Math.* **41** (1910) 193–203.

18. A. J. Kempner, Polynomials and their residue systems, *Trans. Amer. Math. Soc.* **22** (1921) 240–288.
19. N. Koblitz, q-Extension of the p-adic Gamma function, *Trans. Amer. Math. Soc.* **260** (1980) 449–457.
20. D. A. Lind, Which polynomials over an algebraic number field map the algebraic integers into themselves?, *Amer. Math. Monthly* **78** (1971) 179–180.
21. K. Mahler, An interpolation series for a continuous function of a p-adic variable, *J. reine angew. Math.* **199** (1958) 23–34.
22. D. Maulik, Root sets of polynomials modulo prime powers, preprint.
23. D. L. McQuillan, On a Theorem of R. Gilmer, *J. Number Theory* **39** (1991) 245–250.
24. J. W. Milnor and J. D. Stasheff, *Characteristic classes*, Annals of Mathematics Studies, No. 76, Princeton University Press, Princeton, N.J., 1974.
25. Y. Morita, A p-adic analogue of the Γ-function, *J. Fac. Sc. University Tokyo* **22** (1975) 255–266.
26. A. Ostrowski, Über ganzwertige Polynome in algebraischen Zahlkörpern, *J. reine angew. Math.* **149** (1919) 117–124.
27. G. Pólya, Über ganzwertige ganze Funktionen, *Rend. Circ. Mat. Palermo* **40** (1915) 1–16.
28. G. Pólya, Über ganzwertige Polynome in algebraischen Zahlkörpern, *J. reine angew. Math.* **149** (1919) 97–116.
29. B. Sury, An integral polynomial, *Math. Mag.* **68** (1995) 134–135.
30. D. S. Thakur, Gamma functions for function fields and Drinfeld modules, *Ann. Math.* **134** (1991) 25–64.
31. D. S. Thakur, On gamma functions for function fields, in *The arithmetic of function fields*, Ohio State Univ. Math. Res. Inst. Publ., 2, de Gruyter, Berlin, 1992, pp. 75–86.

MANJUL BHARGAVA was born in Hamilton, Ontario, Canada, but spent most of his early years in Long Island, New York. He received his A.B. summa cum laude in mathematics from Harvard University in 1996, and his Ph.D. from Princeton University in 2000. His research interests are primarily in number theory, representation theory, and combinatorics, although he also enjoys algebraic geometry, linguistics, and Indian classical music. He was the recipient of the AMS-MAA-SIAM Frank and Brennie Morgan Prize in 1997, and is a Clay Mathematics Institute Long-Term Prize Fellow and a Visiting Fellow at Princeton University.
52 Stewart Avenue, Bethpage, NY 11714-5311
bhargava@math.princeton.edu