INTEGER VALUED POLYNOMIALS AND LUBIN-TATE FORMAL GROUPS

EHUD DE SHALIT AND ERAN ICELAND

Abstract. If R is an integral domain and K is its field of fractions, we let $Int(R)$ stand for the subring of $K[x]$ which maps R into itself. We show that if R is the ring of integers of a p-adic field, then $Int(R)$ is generated, as an R-algebra, by the coefficients of the endomorphisms of any Lubin-Tate group attached to R.

1. Introduction

For an integral domain R, with field of fractions K, we denote by $Int(R)$ the R-subalgebra of $K[x]$ consisting of the polynomials which map R into itself. These polynomials are called R-valued or, sometimes, by abuse of language, integer valued. It is well-known, and easy, that $Int(\mathbb{Z})$ is generated (in fact, linearly spanned) by the binomial coefficients $\binom{x}{n}$. One "explanation" for the fact that these polynomials are integer valued is the following. Consider the multiplicative formal group, as a formal group over $\mathbb{Z}$. Multiplication by x on the formal group is given by a power series whose coefficients are $\binom{x}{n}$. Since for integral x these coefficients must be integral, the binomial coefficients are integer-valued.

Our main theorem is a generalization of this fact to Lubin-Tate groups over the ring of integers R of a p-adic field K (a finite extension of $\mathbb{Q}_p$). If $F(t_1, t_2)$ is a Lubin-Tate formal group law over R, then for every $x \in R$ there is a unique power series

$$[x](t) = [x]_F(t) = \sum_{n=1}^{\infty} c_n(x) t^n \tag{1.1}$$

such that $F([x](t_1), [x](t_2)) = [x](F(t_1, t_2))$ and $c_1(x) = x$. It turns out that $c_n(x) \in K[x]$ is an integer valued polynomial of degree $\leq n$ and what we show is that they generate $Int(R)$ as an R-algebra:

$$Int(R) = R[c_1, c_2, \ldots]. \tag{1.2}$$

In fact, it follows from our proof that $c_1, c_q, c_{q^2,\ldots}$ is a minimal set of generators for $Int(R)$, where q is the cardinality of the residue field of R. For global applications it is nevertheless better to keep all the c_n.

The theory of elliptic curves with complex multiplication and an easy localization argument allow us to apply our result to determine a system of "natural" generators for $Int(R)$ when R is the ring of S-integers in a quadratic imaginary field of class number 1, and S is an explicit small set of primes.

Date: April 22, 2008.
Key words and phrases. Integer valued polynomials, formal groups.

The ring $Int(R)$ is in general non-noetherian, and has been studied by several authors, beginning with Pólya and Ostrowski in 1919. The case of $Int(\mathbb{Z})$ is of course much older, and must have been known to Euler. For a comprehensive survey, see the book [Ca-Ch1], and the recent paper [Ca-Ch2] by the same authors. We thank the referee for calling our attention to past work, which we now briefly summarize, in order to put our result in a historic perspective.

For R the ring of integers of a number field K, $Int(R)$ is a free R-module, as follows from a general theorem of Bass (see [Za], Section 2). Of special interest are number fields K for which $Int(R)$ admits an R-basis $\{f_n\}$ with $\deg(f_n) = n$. Such a basis is called a *regular basis.* Pólya [Po] remarked that a regular basis exists if and only if for every $n \geq 0$, the fractional ideal $\mathfrak{a}_n$ of leading coefficients of polynomials of degree $\leq n$ in $Int(R)$ is principal, and proved that if K is *quadratic* this happens if and only if all the ramified primes in K are principal. In a paper published back-to-back with Pólya's paper, Ostrowski [Os] proved the following more general criterion: $Int(R)$ admits a regular basis if and only if for every rational prime power q, the ideal

$$\prod_{\mathbf{N}\mathfrak{p}=q} \mathfrak{p} \tag{1.3}$$

(the product extending over all the prime ideals of R of absolute norm q) is principal. The subgroup of the ideal class group of K generated by the classes of these ideals is called the *Pólya-Ostrowski group* of R, and may be regarded as the obstruction to $Int(R)$ possessing a regular basis. If $K/\mathbb{Q}$ is Galois, it is enough to check Ostrowski's criterion for $q = p^f$ where p is ramified in K. In this case Zantema [Za, Prop. 3.1] found an equivalent formulation of the criterion in terms of $H^1(G, U)$ where $G = Gal(K/\mathbb{Q})$ and $U = R^\times$ is the group of units of K. Number fields of class number 1 evidently admit a regular basis for $Int(R)$, but so do many others, for example all the cyclotomic fields $\mathbb{Q}(e^{2\pi i/m})$.

All of the above concerns bases of $Int(R)$ as an R-module. The question of finding generators *as an R-algebra,* addressed by us, seemed to have escaped attention. So did, to the best of our knowledge, the relation with formal groups, although the quantities $w_q(n)$, which play a key role in our proof, show up in various circumstances.

We end our brief historic survey with the remark that there are other aspects of the ring $Int(R)$ which make it an object worth studying. For example, if R is the ring of integers of a number field, $Int(R)$ is a two-dimensional Prüfer domain. There are analogous results of Carlitz in the function-field case. We refer to the paper of Cahen and Chabert for a list of known results and open problems.

2. Integer valued polynomials

2.1. **General facts.** As in the introduction, let R be an integral domain, K its field of fractions, and

$$Int(R) = \{f \in K[x] | \, f(R) \subset R\} \tag{2.1}$$

$$Int_n(R) = \{f \in Int(R) | \, \deg(f) \leq n\} \tag{2.2}$$

$$\mathfrak{a}_n(R) = \{\text{leading coefficients of } f \in Int_n(R)\}. \tag{2.3}$$

Clearly $Int(R)$ is an R-subalgebra of $K[x]$, and $\mathfrak{a}_n(R)$ is an R-submodule (a fractional ideal) of K. It is also clear that if R is a principal ideal domain then $Int(R)$

has a basis $\{f_n\}_{n\geq 0}$ over R such that $\deg(f_n) = n$ (a *regular basis*) and that f_n is unique up to multiplication by a unit of R and a linear combination of $f_0, \dots, f_{n-1}$. In fact, any f_n whose leading coefficient generates $\mathfrak{a}_n(R)$ will do.

We next examine the effect of localization, under the mere assumption that R is a noetherian domain. For any prime $\mathfrak{p}$ of R,

$$Int(R)_{\mathfrak{p}} = Int(R_{\mathfrak{p}}) \tag{2.4}$$

(as submodules of $K[x]$, see [Ca-Ch1], Theorem I.2.3). Let $\mathcal{M}$ be the collection of maximal ideals of R. It follows that

$$Int(R) = \bigcap_{\mathfrak{p}\in\mathcal{M}} Int(R_{\mathfrak{p}}). \tag{2.5}$$

Indeed, let f belong to the right hand side, and let I be the ideal of all $a \in R$ such that $af \in Int(R)$. For every $\mathfrak{p} \in \mathcal{M}$, from the fact that $f \in Int(R_{\mathfrak{p}}) = Int(R)_{\mathfrak{p}}$ we learn that there is an $a \in I$, $a \notin \mathfrak{p}$. Thus I is contained in no maximal ideal, so must contain 1.

We shall also need the following lemma, whose easy proof we leave out.

Lemma 2.1. *Let $Q \subset P \subset K[x]$ be two R-submodules and let $\mathfrak{a}_n(Q)$ denote the set of leading coefficients of polynomials of degree n in Q. If $\mathfrak{a}_n(Q) = \mathfrak{a}_n(P)$ for all $n \geq 0$, then $Q = P$.*

2.2. **Integer valued polynomials over discrete valuation ring.** Assume now that R is a discrete valuation ring, let π be a uniformizer, and v the normalized valuation, so that $v(\pi) = 1$. If the residue field of R is infinite, it is easy to see that $Int(R) = R[x]$. Assume therefore that the cardinality of $R/\pi R$ is finite, and denote it by q.

Let

$$w_q(n) = \left\lfloor \frac{n}{q} \right\rfloor + \left\lfloor \frac{n}{q^2} \right\rfloor + \left\lfloor \frac{n}{q^3} \right\rfloor + \cdots \tag{2.6}$$

(see [Ca-Ch2] for the history of these numbers, going back to Legendre and ending with recent work of Bhargava). Below we shall use the fact that

$$w_q(i_1) + \cdots + w_q(i_l) \leq w_q(i_1 + \cdots + i_l), \tag{2.7}$$

and that the inequality is *strict* if $l \geq 2$, all the $i_j \geq 1$ and $i_1 + \cdots + i_l = q^m$ for some m.

Proposition 2.2. *We have*

$$\mathfrak{a}_n(R) = \pi^{-w_q(n)}R. \tag{2.8}$$

Proof. See [Ca-Ch2], Proposition 1.3, or [Za], Lemma 2.2. □

3. Relation with Lubin Tate formal groups

Let K be a finite extension of $\mathbb{Q}_p$ with ring of integers R. As before let π be a uniformizer, and denote by q the cardinality of $\kappa = R/\pi R$. Let F be a Lubin-Tate formal group law over R associated with the uniformizer π [L-T]. As in the introduction, to every $x \in R$ we can associate a unique endomorphism $[x]$ of F of the form

$$[x](t) = xt + c_2(x)t^2 + c_3(x)t^3 + \cdots \in R[[t]]. \tag{3.1}$$

Using the logarithm of the formal group F it is easy to see that $c_n(x) \in K[x]$ is a polynomial of degree $\leq n$. Since it is R-valued, $c_n \in Int(R)$.

In particular

$$[\pi](t) = \pi t + a_2 t^2 + \cdots + a_q t^q + \cdots \tag{3.2}$$

lifts the Frobenius endomorphism: it satisfies $a_i \equiv 0 mod \pi$ for $i \neq q$, and $a_q \equiv 1 mod \pi$. Let $u = a_q$.

Theorem 3.1. *We have*

$$R[c_1, c_2, \ldots] = Int(R). \tag{3.3}$$

Moreover, $\{c_{q^m} \,|\, m \geq 0\}$ *is a minimal set of generators of* $Int(R)$ *as an* R*-algebra.*

Proof. Let $Q = R[c_1, c_q, c_{q^2}, \ldots]$. From the lemma and the proposition we deduce that in order to prove that $Q = Int(R)$ it is enough to show that

$$\pi^{-w_q(n)} R \subset \mathfrak{a}_n(Q) \tag{3.4}$$

for every $n \geq 0$.

If we expand $n = b_m q^m + b_{m-1} q^{m-1} + \cdots + b_1 q + b_0$ with $0 \leq b_i < q$, we see that

$$w_q(n) = b_m w_q(q^m) + b_{m-1} w_q(q^{m-1}) + \cdots + b_1 w_q(q) \tag{3.5}$$

where $w_q(q^m) = (q^m - 1)/(q - 1)$ $(m \geq 1)$. Let λ_n be the coefficient of x^n in $c_n(x)$. Then the coefficient of x^n in $c_{q^m}^{b_m} c_{q^{m-1}}^{b_{m-1}} \ldots c_q^{b_1} c_1^{b_0}$ (which is a polynomial of degree n in Q) is

$$\lambda_{q^m}^{b_m} \lambda_{q^{m-1}}^{b_{m-1}} \ldots \lambda_q^{b_1} \lambda_1^{b_0}. \tag{3.6}$$

It follows that it is enough to prove that

$$v(\lambda_{q^m}) = -w_q(q^m) \tag{3.7}$$

for every $m \geq 0$. Since $\lambda_1 = 1$, this holds for $m = 0$.

From $[\pi x](t) = [\pi]([x](t))$ we derive the *basic identity*

(3.8)

$$\sum c_n(\pi x) t^n = \pi \left(\sum c_n(x) t^n \right) + a_2 \left(\sum c_n(x) t^n \right)^2 + \cdots + u \left(\sum c_n(x) t^n \right)^q + \cdots$$

Comparing coefficients of $x^q t^q$ we get

$$\lambda_q(\pi^q - \pi) = a_2(2\lambda_1 \lambda_{q-1} + \cdots) + a_3(\cdots) + \cdots + u. \tag{3.9}$$

In this last equation, $v(LHS) = v(\lambda_q) + 1$. On the right hand side, each term is of the form $a_l \lambda_{i_1} \lambda_{i_2} \ldots \lambda_{i_l}$ where $l \geq 2$ and $i_1 + i_2 + \cdots + i_l = q$. Since $v(\lambda_{i_j}) \geq 0$, and $v(a_l) \geq 1$, unless $l = q$ and $a_q = u$, we deduce that $v(RHS) = v(u) = 0$. Hence $v(\lambda_q) = -1$, as we wanted to show.

We will now prove that $v(\lambda_{q^m}) = -w_q(q^m)$ by induction on m, the cases $m = 0$ and 1 having been proved above. Suppose that $v(\lambda_{q^{m-1}}) = -w_q(q^{m-1})$. Note also:

- For each n, $v(\lambda_n) \geq -w_q(n)$ (because $\lambda_n \in \mathfrak{a}_n(R)$).
- If $i_1 + i_2 + \cdots + i_l = q^m$ then $w_q(i_1) + \cdots + w_q(i_l) < w_q(q^m)$ (we assume here that the $i_j \geq 1$ and $l \geq 2$).

Comparing the coefficients of $x^{q^m}t^{q^m}$ in the basic identity, as we did when m was 1, yields

$$\begin{aligned} \lambda_{q^m}(\pi^{q^m}-\pi) &= a_2(\sum_{i_1+i_2=q^m}\lambda_{i_1}\lambda_{i_2}) + a_3(\sum_{i_1+i_2+i_3=q^m}\lambda_{i_1}\lambda_{i_2}\lambda_{i_3}) + \cdots \\ &\quad + u(\sum_{i_1+\cdots+i_q=q^m}\lambda_{i_1}\lambda_{i_2}\ldots\lambda_{i_q}) + a_{q+1}(\cdots) + \cdots \end{aligned} \tag{3.10}$$

The valuation of the left hand side, $v(LHS) = v(\lambda_{q^m}) + 1$. The right hand side is a sum of terms of the form $a_l\lambda_{i_1}\lambda_{i_2}\ldots\lambda_{i_l}$ where $l \geq 2$ and $i_1+\cdots+i_l = q^m$. We shall show that the term $u\lambda^q_{q^{m-1}}$ has strictly smaller valuation than any other term, so

$$v(RHS) = v(u\lambda^q_{q^{m-1}}) = -qw_q(q^{m-1}) \tag{3.11}$$

by the induction hypothesis, and $v(\lambda_{q^m}) = -1 - qw_q(q^{m-1}) = -w_q(q^m)$.

To conclude the proof we examine a term of the form $a_l\lambda_{i_1}\lambda_{i_2}\ldots\lambda_{i_l}$, other than $u\lambda^q_{q^{m-1}}$, distinguishing two cases. If $l \neq q$

$$v(a_l\lambda_{i_1}\lambda_{i_2}\ldots\lambda_{i_l}) \geq 1 - w_q(i_1) - \cdots - w_q(i_l) > 1 - w_q(q^m) = -qw_q(q^{m-1}). \tag{3.12}$$

If $l = q$ but not all the i_j are equal to q^{m-1}, then without loss of generality $i_1 < q^{m-1}$. We shall show shortly that in this case

$$w_q(i_1) + \cdots + w_q(i_q) < qw_q(q^{m-1}) \tag{3.13}$$

so that once again

$$v(u\lambda_{i_1}\lambda_{i_2}\ldots\lambda_{i_q}) \geq -w_q(i_1) - \cdots - w_q(i_q) > -qw_q(q^{m-1}). \tag{3.14}$$

Assume therefore that $i_1+\cdots+i_q = q^m$ and $i_1 < q^{m-1}$. This implies $\left\lfloor \frac{i_1}{q^{m-1}} \right\rfloor = 0$. By definition

$$w_q(i_j) = \left\lfloor \frac{i_j}{q} \right\rfloor + \left\lfloor \frac{i_j}{q^2} \right\rfloor + \cdots + \left\lfloor \frac{i_j}{q^{m-1}} \right\rfloor. \tag{3.15}$$

Therefore, recalling that $\sum\lfloor x_j \rfloor \leq \lfloor \sum x_j \rfloor$,

$$\begin{aligned} w_q(i_1) + \cdots + w_q(i_q) &= \sum_{j=1}^{q}\left\lfloor \frac{i_j}{q} \right\rfloor + \sum_{j=1}^{q}\left\lfloor \frac{i_j}{q^2} \right\rfloor + \cdots + \sum_{j=1}^{q}\left\lfloor \frac{i_j}{q^{m-2}} \right\rfloor + \sum_{j=2}^{q}\left\lfloor \frac{i_j}{q^{m-1}} \right\rfloor \\ &\leq \left\lfloor \frac{q^m}{q} \right\rfloor + \left\lfloor \frac{q^m}{q^2} \right\rfloor + \cdots + \left\lfloor \frac{q^m}{q^{m-2}} \right\rfloor + \left\lfloor \frac{q^m - i_1}{q^{m-1}} \right\rfloor \\ &< q^{m-1} + q^{m-2} + \cdots + q^2 + q = qw_q(q^{m-1}). \end{aligned} \tag{3.16}$$

This concludes the proof that $Q = Int(R)$. It remains to see that no c_{q^m} can be eliminated from the set of generators of Q. Suppose $b_i \geq 0$ and

$$q^m = b_{m-1}q^{m-1} + b_{m-2}q^{m-2} + \cdots + b_1q + b_0. \tag{3.17}$$

The leading coefficient of $c^{b_{m-1}}_{q^{m-1}} \ldots c^{b_1}_q c^{b_0}_1$ has valuation

$$-b_{m-1}w_q(q^{m-1}) - \cdots - b_1w_q(q) > -w_q(q^m), \tag{3.18}$$

so we need c_{q^m} to guarantee that $\mathfrak{a}_{q^m}(Q) = \pi^{-w_q(q^m)}R$. □

4. Global applications

4.1. **Applications to elliptic curves with complex multiplication.** Let K be a quadratic imaginary field of class number 1. Let $\mathcal{O}_K$ be its ring of integers, and E/K an elliptic curve with complex multiplication by the ring $\mathcal{O}_K$. Pick a Weierstrass equation for E defined over K,

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6. \tag{4.1}$$

Let $t = -X/Y$ be the local parameter at the origin as defined in [Si, chapter IV] and

$$[x]_{\widehat{E}}(t) = xt + c_2(x)t^2 + c_3(x)t^3 + \cdots \ (x \in \mathcal{O}_K) \tag{4.2}$$

the power series giving the multiplication by x in the formal group. Then $c_n(x) \in K[x]$ is of degree $\leq n$. Let S be a finite set of primes such that if $\mathfrak{p} \notin S$ the chosen Weierstrass model is integral and has good reduction at $\mathfrak{p}$. Let $R = \mathcal{O}_{K,S}$ be the ring of S-integers in K. At a prime $\mathfrak{p} \notin S$ the formal group of E is Lubin-Tate, and $c_n(x) \in R_{\mathfrak{p}} = \mathcal{O}_{K,\mathfrak{p}}$. Our main theorem yields

$$Int(R_{\mathfrak{p}}) = R_{\mathfrak{p}}[c_1, c_2, c_3, ...]. \tag{4.3}$$

From $Int(R) = \bigcap_{\mathfrak{p}\notin S} Int(R_{\mathfrak{p}})$ we deduce:

Corollary 4.1. *Under the conditions mentioned above, $Int(R)$ is generated over R by the $c_n(x)$.*

In fact it is enough to take c_n for $n's$ which are powers of cardinalities of residue fields of R.

Example. Let E be the elliptic curve given, in Weierstrass form, by $Y^2 = X^3 - X$. This model has complex multiplication by $\mathbb{Z}[i]$ and good reduction everywhere away from 2. We may therefore apply the corollary to the ring $\mathbb{Z}[i, \frac{1}{2}]$. By a simple computation we find that the polynomials $c_n(x)$ vanish for $n \neq 1 mod 4$. The first few non-vanishing polynomials are

$c_1(x) = x$
$c_5(x) = \frac{2}{5}(x^5 - x)$
$c_9(x) = \frac{2}{15}x^9 - \frac{4}{5}x^5 + \frac{2}{3}x$
$c_{13}(x) = \frac{44}{975}x^{13} - \frac{12}{25}x^9 + \frac{148}{75}x^5 - \frac{20}{13}x$
$c_{17}(x) = \frac{39422}{27625}x^{17} - \frac{88}{375}x^{13} + \frac{196}{125}x^9 - \frac{26648}{4875}x^5 + \frac{46}{17}x$

Note that the next in line, $c_{21}(x)$, is redundant, according to the remark following the corollary.

4.2. **Formal globalization.** As pointed out by the referee, the use of complex multiplication, as much as it points to a relation between our problem and geometry, is not essential. We only need to know a one-dimensional formal group over R, admitting R as endomorphisms, all of whose localizations are Lubin-Tate formal groups. This can be done much more generally with little effort.

Let K be any number field, and S a finite set of primes such that $R = \mathcal{O}_{K,S}$ is of class number 1 (S may be empty). For any prime $\mathfrak{p} \notin S$ let $\pi_{\mathfrak{p}} \in R$ be a generator of $\mathfrak{p}R$. Consider the formal Dirichlet series

$$\begin{aligned} L(s) &= \prod_{\mathfrak{p}\notin S} \left(1-\pi_{\mathfrak{p}}^{-1}\mathbb{N}\mathfrak{p}^{-s}\right)^{-1} \\ &= \sum_{n=1}^{\infty} a_n n^{-s}. \end{aligned} \tag{4.4}$$

Clearly $a_1 = 1$ and $a_n \in K$. For every $\mathfrak{p} \notin S$, the Dirichlet series $\left(1-\pi_{\mathfrak{p}}^{-1}\mathbb{N}\mathfrak{p}^{-s}\right) L(s)$ has $\mathfrak{p}$-integral coefficients. Consider the formal power series

$$f(X) = \sum_{n=1}^{\infty} a_n X^n \tag{4.5}$$

and the group law

$$F(X,Y) = f^{-1}(f(X)+f(Y)) \tag{4.6}$$

for which f is a logarithm. A priori F is defined over K, but we claim that it is in fact defined over R. For every $\mathfrak{p} \notin S$

$$f(X) - \pi_{\mathfrak{p}}^{-1} f(X^{\mathbb{N}\mathfrak{p}}) \in \mathcal{O}_{K,\mathfrak{p}}[[X]]. \tag{4.7}$$

To see this, we must show that, if $\mathbb{N}\mathfrak{p} = q$, $a_n - \pi_{\mathfrak{p}}^{-1} a_{n/q} \in \mathcal{O}_{K,\mathfrak{p}}$ (if q does not divide n, we understand $a_{n/q} = 0$). But this is guaranteed by the fact that $\left(1-\pi_{\mathfrak{p}}^{-1}\mathbb{N}\mathfrak{p}^{-s}\right) L(s)$ has $\mathfrak{p}$-integral coefficients. The functional equation lemma [Haz, I.2.2] implies now that F has coefficients in $\mathcal{O}_{K,\mathfrak{p}}$, and that so does the endomorphism

$$[x]_F(t) = f^{-1}(xf(t)) \tag{4.8}$$

for every $x \in \mathcal{O}_{K,\mathfrak{p}}$. Furthermore, by [Haz, I.8.3.6] F is a Lubin-Tate formal group law associated with the prime $\pi_{\mathfrak{p}}$.

It follows that F, as well as the endomorphisms $[x]_F$, for $x \in R$, are defined over R, and therefore that the Taylor coefficients $c_n(x)$ in $[x]_F$ belong to $Int(R)$. Moreover, by our main theorem, they generate $Int(R_{\mathfrak{p}})$ at each maximal ideal $\mathfrak{p}$, so we may deduce as before that they generate $Int(R)$ globally.

References

[Ca-Ch1] Cahen, P.-J., Chabert, J.-L., *Integer-valued polynomials,* AMS Surveys and Monographs **48,** Providence, 1997.

[Ca-Ch2] Cahen, P.-J., Chabert, J.-L., *Old problems and new questions around integer-valued polynomials and factorial sequences,* in *Multiplicative ideal theory in commutative algebra, a tribute to Robert Gilmore,* Springer-Verlag, New-York, 2006, p.89-108.

[Haz] Hazewinkel, M., *Formal groups and applications,* Academic Press, New York, 1978.

[L-T] Lubin, J., Tate, J., *Formal complex multiplication in local fields,* Annals of Math. **81** (1965), 380-387.

[Os] Ostrowski, A., *Über ganzwertige Polynome in algebraischen Zahlkörpren*, J. Reine Angew. Math. **149** (1919), 117-124.

[Po] Pólya, G., *Über ganzwertige Polynome in algebraischen Zahlkörpren*, J. Reine Angew. Math. **149** (1919), 97-116.

[Si] Silverman, J.H., *The arithmetic of elliptic curves,* GTM **106**, Springer-Verlag, New York, 1986.

[Za] Zantema, H., *Integer valued polynomials over a number field*, Manuscripta Math. **40** (1982), 155-203.

Hebrew University, Jerusalem, Israel
E-mail address: deshalit@math.huji.ac.il

Hebrew University, Jerusalem, Israel
E-mail address: iceland@math.huji.ac.il