A p-adic Euclidean Algorithm

Cortney Lager
Winona State University

October 20, 2009

1 Introduction

The rational numbers can be completed with respect to the standard absolute value and this produces the real numbers. However, there are other absolute values on the rationals besides the standard one. Completing the rationals with respect to one of these produces the p-adic numbers. In this paper, we take some basic number theory concepts and apply them to rational p-adic numbers. Using these concepts, a p-adic division algorithm is developed along with a p-adic Euclidean Algorithm. These algorithms produce a generalized greatest common divisor in the p-adics along with a p-adic simple continued fraction. In Section 2, we describe the p-adic numbers, and in Section 3 we present our p-adic Division Algorithm and Euclidean Algorithm. In Section 4, we show some applications, including a connection to Browkin's p-adic continued fractions, which motivatored our investigations in the first place. Finally, in Section 5, we give some open questions for further study.

2 p-adic Numbers

Since we will use different absolute value functions in this paper, to avoid confusion we will denote the standard absolute value as $|\cdot|_\infty$ rather than $|\cdot|$. For each prime p there exists an absolute value on the rationals $|\cdot|_p : \mathbb{Q} \to \mathbb{Q}$ defined by

$$\left|\frac{a}{b}\right|_p = p^{v(b)-v(a)}$$

where $v(n)$ is the number of times p divides the integer n. Also $|0|_p = 0$. This is called a p-adic absolute value, and in the context of measuring the size of a number (i.e. its distance to zero), it states that the more a rational number is divisible by p, the smaller it is. For example,

$$|162|_3 = 3^{-4} < \left|\frac{5}{27}\right|_3 = 3^3.$$

So 162 is "smaller" than $\frac{5}{27}$ in the 3-adics.

Completing the rationals with respect to the p-adic absolute value yields $\mathbb{Q}_p$, the p-adic numbers. Let p be an odd prime for the remainder of the paper. Then there are a few different ways to think about p-adic numbers ([2],[3], [4], [5]) but for the purposes of this paper we will consider them in the following way.

Definition 1. *An element $\zeta \in \mathbb{Q}_p$ is a Laurent series in the odd prime p,*

$$\zeta = \sum_{j=m}^{\infty} c_j p^j = c_m p^m + c_{m+1} p^{m+1} + c_{m+2} p^{m+2} + \dots \tag{1}$$

where m is a (possibly negative) integer and $c_j \in \left\{\frac{1-p}{2}, \dots, \frac{p-1}{2}\right\}$.

Note that in the standard absolute value, the p-series in (1) would only converge if it had a finite number of terms. However, under the p-adic absolute value, each term is in fact getting smaller, and it can be shown [3] that all such infinite Laurent series in p converge under the p-adic absolute value. It's also worth noting that the rational numbers are a subset of the p-adics, although they are slightly disguised. For example, $1/2$ in the 7-adics is given by the power series

$$4 + 3 \cdot 7 + 3 \cdot 7^2 + 3 \cdot 7^3 + \cdots .$$

Since the geometric series test still applies to the p-adic absolute value and to convergence in $\mathbb{Q}_p$, then it gives the following,

$$4 + 3 \cdot 7 + 3 \cdot 7^2 + 3 \cdot 7^3 + \cdots = 1 + 3\left(\frac{1}{1-7}\right) = \frac{1}{2}.$$

For the remainder of the paper we will use the fractional representation instead of the p-series for rationals elements of $\mathbb{Q} \subset \mathbb{Q}_p$.

Using the notation in (1), we can define $v(\zeta) = m$, thus $|\zeta|_p = p^{-m}$. Further, every $\zeta \in \mathbb{Q}_p \backslash \{0\}$ can be written as $\zeta = up^{\epsilon}$, where $\epsilon = v(\zeta)$ and $|u|_p = 1$. We also have the standard properties of a non-archimedean norm:

$$|\zeta_1 \zeta_2|_p = |\zeta_1|_p |\zeta_2|_p \quad \text{and} \quad |\zeta_1 + \zeta_2|_p \leq \max(|\zeta_1|_p, |\zeta_2|_p).$$

The non-archimedean triangle inequality gives equality if $|\zeta_1|_p \neq |\zeta_2|_p$.

3 The p-adic Division Algorithm and Euclidean Algorithm

Both the division algorithm and the Euclidean algorithm are elements of classical number theory. With the goal of recreating the real aspects of classical number theory in the p-adics, we now re-invent these two important classical algorithms. Let $\mathbb{Z}\left[\frac{1}{p}\right] = \left\{\frac{m}{p^k} \mid m,\ k \in \mathbb{Z}\right\}$. Notice that $\mathbb{Z}\left[\frac{1}{p}\right]$ is closed under addition and multiplication; in fact, it is a subring of $\mathbb{Q}$.

Theorem 1 (p-adic Division Algorithm)**.** *Let p be an odd prime. Then given any σ and $\tau \in \mathbb{Q}_p$ where $\tau \neq 0$, there exists uniquely $q \in \mathbb{Z}\left[\frac{1}{p}\right]$ with $|q|_\infty < \frac{p}{2}$, and $\eta \in \mathbb{Q}_p$ with $|\eta|_p < |\tau|_p$ such that*

$$\sigma = q\tau + \eta.$$

Proof. If $|\sigma|_p < |\tau|_p$, then let $q = 0$ and $\eta{=}\sigma$. Otherwise, write $\sigma{=}sp^{v(\sigma)}$, $\tau{=}tp^{v(\tau)}$ where $|s|_p = |t|_p = 1$. Let

$$q = \overline{q}p^{v(\sigma)-v(\tau)},$$

where $\overline{q} \in \mathbb{Z}$ such that $\overline{q} \equiv st^{-1} \bmod p^{v(\tau)-v(\sigma)+1}$ and $|\overline{q}|_\infty < p^{v(\tau)-v(\sigma)+1}/2$. Then $|q|_\infty < \frac{p}{2}$. Then let $\eta = sp^{v(\sigma)} - qtp^{v(\tau)} = (s - \overline{q}t)p^{v(\sigma)}$. Thus, $v(\tau) + 1 \leq v(\eta)$ and therefore $|\eta|_p < |\tau|_p$.

To prove uniqueness, suppose $\sigma = \tau q + \eta = \tau q' + \eta'$ where $q = \frac{m}{p^k}$, and $q' = \frac{m'}{p^k}$. Then, $\tau(q - q') = \eta' - \eta$. Thus,

$$|\tau|_p|q - q'|_p = |\tau(q - q')|_p = |\eta' - \eta|_p \leq \max(|\eta|_p, |\eta'|_p) < |\tau|_p,$$

which implies that $p \mid q - q' = \frac{m-m'}{p^k}$. Thus, $p^{k+1} \mid m - m'$. However, since $|q - q'|_\infty < p$, then $|m - m'|_\infty < p^{k+1}$. Hence, $m = m'$, $q = q'$, and $\eta = \eta'$. □

Note in the proof of Theorem 1 that if $q \neq 0$, then in fact $p \nmid \overline{q}$, and therefore $v(q) = v(\sigma) - v(\tau) \leq 0$; that is $|q|_p \geq 1$.

Since we now have a division algorithm in the p-adics, we can iterate the process in a way similar to the classical Euclidean Algorithm.

Definition 2 (p-adic Euclidean Algorithm)**.** *Let p be an odd prime. The p-adic Euclidean Algorithm applied to σ and $\tau \in \mathbb{Q}_p$ and where $\tau \neq 0$ is as follows. First, apply Theorem 1 to σ and τ to produce*

$$\sigma = q_1\tau + \eta_1. \tag{2}$$

In each subsequent step "shift to the left" and apply Theorem 1 again,

$$\begin{aligned} \tau &= q_2\eta_1 + \eta_2 \\ \eta_1 &= q_3\eta_2 + \eta_3 \\ &\vdots \\ \eta_{i-2} &= q_i\eta_{i-1} + \eta_i \\ &\vdots \end{aligned} \tag{3}$$

This process either continues indefinitely or stops when $\eta_i = 0$. The outputs of this algorithm are the sequences $\{q_i\}$ and $\{\eta_i\}$. When appropriate we will consider the inputs as $\sigma = \eta_{-1}$ and $\tau = \eta_0$.

Example. The 7-adic Euclidean Algorithm applied to $\frac{181625}{11}$ and $\frac{10555}{2}$ yields

$$\begin{aligned}
\frac{181625}{11} &= (2)\left(\frac{10555}{2}\right) + \left(\frac{9360}{11}\cdot 7^1\right) \\
\frac{10555}{2} &= \left(\frac{12}{7}\right)\left(\frac{9360}{11}\cdot 7^1\right) + \left(\frac{-2215}{22}\cdot 7^2\right) \\
\frac{9360}{11}\cdot 7^1 &= \left(\frac{-10}{7}\right)\left(\frac{-2215}{22}\cdot 7^2\right) + \left(\frac{-5}{11}\cdot 7^4\right) \\
\frac{-2215}{22}\cdot 7^2 &= \left(\frac{50}{7^2}\right)\left(\frac{-5}{11}\cdot 7^4\right) + \left(\frac{-5}{22}\cdot 7^5\right) \\
\frac{-5}{11}\cdot 7^4 &= \left(\frac{2}{7}\right)\left(\frac{-5}{22}\cdot 7^5\right) + 0.
\end{aligned}$$

The algorithm stops since $\eta_5 = 0$. The outputs are the sequences

$$\{q_i\} = \left\{2, \frac{12}{7}, \frac{-10}{7}, \frac{50}{7^2}, \frac{2}{7}\right\}$$

and

$$\{\eta_i\} = \left\{\frac{9360}{11}\cdot 7^1, \frac{-2215}{22}\cdot 7^2, \frac{-5}{11}\cdot 7^4, \frac{-5}{22}\cdot 7^5\right\}.$$

Lemma 1. *Let η_i be the outputs from the p-adic Euclidean Algorithm of $\sigma = \frac{a}{b}p^{v(\sigma)} \in \mathbb{Q}$, $\tau = \frac{c}{d}p^{v(\tau)} \in \mathbb{Q}$ when $\frac{a}{b}$ and $\frac{c}{d}$ are in lowest terms. Then $lcm(b,d)\cdot \eta_i \in \mathbb{Z}\left[\frac{1}{p}\right]$.*

Proof. Let $l = \text{lcm}(b,d)$. From multiplying through by l in (2),

$$\frac{la}{b}p^{v(\sigma)} = \frac{q_1 lc}{d}p^{v(\tau)} + l\eta_1.$$

Since $\frac{la}{b}p^{v(\sigma)}$, $\frac{q_1 lc}{d}p^{v(\tau)} \in \mathbb{Z}\left[\frac{1}{p}\right]$ then $l\eta_1 \in \mathbb{Z}\left[\frac{1}{p}\right]$.

Then, inductively

$$l\eta_{i-2} = q_i l\eta_{i-1} + l\eta_i$$

with $l\eta_{i-2}$, $q_i l\eta_{i-1} \in \mathbb{Z}\left[\frac{1}{p}\right]$. Thus, $l\eta_i \in \mathbb{Z}\left[\frac{1}{p}\right]$. □

Theorem 2. *Let p be an odd prime and $\sigma, \tau \in \mathbb{Q}$ with $\tau \neq 0$. Then the p-adic Euclidean Algorithm applied to σ and τ has a finite number of steps.*

Proof. For all i such that $q_i, \eta_i \neq 0$, write $\eta_i = h_i p^{\epsilon_i}$ and $q_i = c_i p^{\delta_i}$ where $\epsilon_i = v(\eta_i), \delta_i = v(q_i)$, and $|h_i|_p = |c_i|_p = 1$. Then we have the following.

(i.) By Theorem 1 and the note afterwards, $v(q_i) = v(\eta_{i-2}) - v(\eta_{i-1})$. Thus $\delta_i = \epsilon_{i-2} - \epsilon_{i-1}$.

(ii.) Also, $\epsilon_i \geq \epsilon_{i-1} + 1$ which implies $\epsilon_i > \epsilon_{i-2}$, and

(iii.) $|c_i|_\infty < \frac{p^{1-\delta_i}}{2}$ since $|c_i p^{\delta_i}|_\infty < \frac{p}{2}$.

Then by (3), $h_i = p^{\epsilon_{i-2}-\epsilon_i}(h_{i-2} - c_i h_{i-1})$, where $h_i, c_i \in \mathbb{Q} \subseteq \mathbb{Q}_p$, and therefore

$$\begin{aligned}
|h_i|_\infty &\leq p^{\epsilon_{i-2}-\epsilon_i}(|h_{i-2}|_\infty + |c_i|_\infty |h_{i-1}|_\infty) && \text{by the Triangle Inequality} \\
&< p^{\epsilon_{i-2}-\epsilon_i}(|h_{i-2}|_\infty + \tfrac{1}{2}p^{1-\delta_i}|h_{i-1}|_\infty) && \text{by (iii.)} \\
&= p^{\epsilon_{i-2}-\epsilon_i}(|h_{i-2}|_\infty + \tfrac{1}{2}p^{1+\epsilon_{i-1}-\epsilon_{i-2}}|h_{i-1}|_\infty) && \text{by (i.)} \\
&= p^{\epsilon_{i-2}-\epsilon_i}|h_{i-2}|_\infty + \tfrac{1}{2}p^{1-\epsilon_i+\epsilon_{i-1}}|h_{i-1}|_\infty \\
&< \tfrac{1}{2}|h_{i-2}|_\infty + \tfrac{1}{2}|h_{i-1}|_\infty && \text{by (ii.).}
\end{aligned}$$

Thus, $|h_i|_\infty < \frac{1}{2}|h_{i-2}|_\infty + \frac{1}{2}|h_{i-1}|_\infty$. Now consider the sequence $\{|h_{i-1}|_\infty + 2|h_i|_\infty\} \geq 1$ of positive rational numbers. From the previous inequality,

$$|h_{i-1}|_\infty + 2|h_i|_\infty < |h_{i-2}|_\infty + 2|h_{i-1}|_\infty.$$

Therefore, $|h_{i-1}|_\infty + 2|h_i|_\infty$ is decreasing. If $\sigma = \frac{a}{b}p^{v(\sigma)}$ and $\tau = \frac{c}{d}p^{v(\tau)}$, and $l = \text{lcm}(b, d)$, then, by the Lemma 2.1, $l|h_i|_\infty + 2l|h_{i-1}|_\infty \in \mathbb{Z}$. Therefore, $l|h_i|_\infty + 2l|h_{i-1}|_\infty = 0$ for some finite i and thus the p-adic Euclidean Algorithm has a finite number of steps for rational inputs. □

4 Applications of the p-adic Euclidean Algorithm

4.1 Greatest Common Divisor

Recall the following definition.

Definition 3. *Let a, $b \in \mathbb{Z}$, not both zero. Then the greatest common divisor, or gcd, of a and b is the unique positive integer $g = gcd(a, b)$ that satisfies the following properties.*

(i.) $\frac{a}{g}, \frac{b}{g} \in \mathbb{Z}$, *and*

(ii.) if there exists $f \in \mathbb{Z}$ with $\frac{a}{f}, \frac{b}{f} \in \mathbb{Z}$, then $\frac{g}{f} \in \mathbb{Z}$.

We can extend the definition of the gcd to $t, s \in \mathbb{Q}$, where $t = \frac{a}{b}$ and $s = \frac{c}{d}$ are in lowest terms, by setting

$$\gcd(t, s) = \frac{\gcd(a, c)}{\text{lcm}(b, d)}.$$

This satisfies the properties that if $g = \gcd(t, s)$ then $\frac{t}{g}, \frac{s}{g} \in \mathbb{Z}$ and if there exists $f \in \mathbb{Q}$ with $\frac{t}{g}, \frac{s}{g} \in \mathbb{Z}$, then $\frac{g}{f} \in \mathbb{Z}$.

Recall that the classical Euclidean Algorithm applied to integers a and b computes $\gcd(a, b)$ as the last non-zero remainder. The p-adic Euclidean Algorithm produces a similar computation.

Theorem 3. *Let nonzero $\sigma, \tau \in \mathbb{Q} \subseteq \mathbb{Q}_p$, with $\sigma = sp^{v(\sigma)}$, $\tau = tp^{v(\tau)}$. Suppose the p-adic Euclidean Algorithm applied to σ and τ stops after k steps and let $\eta_i = h_i p^{v(\eta_i)}$. Then $|h_{k-1}|_\infty = \gcd(t, s)$.*

Proof. Since $\eta_{k-2} = q_k \eta_{k-1}$ then $\frac{\eta_{k-2}}{\eta_{k-1}} = q_k \in \mathbb{Z}\left[\frac{1}{p}\right]$ and thus, $\frac{h_{k-2}}{h_{k-1}} \in \mathbb{Z}$. Then, proceeding inductively backwards through the p-adic Euclidean Algorithm,

$$\frac{\eta_{k-2-i}}{\eta_{k-1}} = q_{k-i}\frac{\eta_{k-1-i}}{\eta_{k-1}} + \frac{\eta_{k-i}}{\eta_{k-1}} \in \mathbb{Z}\left[\frac{1}{p}\right].$$

Hence,

$$\frac{s}{h_{k-1}} = \frac{h_{-1}}{h_{k-1}} \in \mathbb{Z} \quad \text{and} \quad \frac{t}{h_{k-1}} = \frac{h_0}{h_{k-1}} \in \mathbb{Z}.$$

Now suppose $f \in \mathbb{Q}$ such that $\frac{t}{f}$, $\frac{s}{f} \in \mathbb{Z}$. Note that $v(f) \leq 0$, since $v(s) = v(t) = 0$, then

$$\frac{h_1 p^{v(\eta_1)}}{f} = \frac{t}{f}p^{v(\tau)} - q_1\frac{s}{f}p^{v(\sigma)} \in \mathbb{Z}[\frac{1}{p}].$$

Thus, $\frac{h_1}{f} \in \mathbb{Z}$. Then again, inductively $\frac{h_{k-1}}{f} \in \mathbb{Z}$. □

Our previous example of the p-adic Euclidean Algorithm shows that

$$\frac{5}{22} = \left(\frac{181625}{11}, \frac{10555}{2}\right).$$

Although this computation may seem trivial when the rational numbers are presented as fractions, all calculations in the p-adic Euclidean algorithm are amenable to elements of $\mathbb{Q}_p$ expressed as in (1).

4.2 Simple Continued Fractions

In addition to the gcd, the classical Euclidean Algorithm also computes the simple continued fraction form of $\frac{a}{b}$:

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots}}} = [q_1, q_2, q_3, \ldots]$$

where $q_i \in \mathbb{Z}$ are the quotients obtained during the Euclidean algorithm. In [1] Browkin defined a simple continued fraction form of a p-adic number, ζ, as follows:

$$\zeta = b_1 + \cfrac{1}{b_2 + \cfrac{1}{b_3 + \cfrac{1}{\ddots}}} = [b_1, b_2, b_3, \ldots]$$

where $b_i \in \mathbb{Q}$ with $|b_i|_\infty < \frac{p}{2}$. The following summarizes Browkin's method.

For ζ with $v(\zeta) = m$ as in (1) define

$$\pi(\zeta) = \begin{cases} 0 & \text{if } m > 0 \\ \sum_{j=m}^{0} c_j p^j & \text{otherwise.} \end{cases}$$

Theorem 4 (Browkin)**.** *Let $\zeta \in \mathbb{Q}_p \backslash \{0\}$, and let $\zeta_1 = \zeta$. For $i \geq 1$, let $b_i = \pi(\zeta_i)$, $\zeta_{i+1} = (\zeta_i - b_i)^{-1}$ until $\zeta_i - b_i = 0$, then $\zeta = [b_1, b_2, b_3, \ldots]$.*

The following theorem relates Browkin's method to the p-adic Euclidean Algorithm. In fact, our proof of Theorem 2 was strongly motivated by the stopping theorem in [1].

Theorem 5. *Let $\zeta \in \mathbb{Q}_p \backslash \{0\}$, and let $\{q_i\}$ be the outputs of the p-adic Euclidean Algorithm applied to ζ and 1. Then $\zeta = [q_1, q_2, q_3, \ldots]$.*

Proof. It suffices to show $q_i = b_i$. However, we will also prove that $\zeta_i = \frac{\eta_{i-2}}{\eta_{i-1}}$. We proceed by induction. In the base case,

$$\zeta_1 = \zeta = \frac{\zeta}{1} = \frac{\eta_{-1}}{\eta_0}.$$

Now, let ζ be as in (1), then

$$|b_1|_\infty = \left| \sum_{j=m}^{0} c_j p^j \right|_\infty \leq \sum_{j=m}^{0} |c_j| p^j \leq \sum_{j=m}^{0} \left(\frac{p-1}{2} \right) p^j$$
$$= \left(\frac{p-1}{2} \right) \sum_{j=m}^{0} p^j = \frac{p-1}{2} \cdot \frac{p - p^m}{p-1} < \frac{p}{2}.$$

Also,

$$|\zeta - b_1|_p = |\zeta_1 - \pi(\zeta_1)|_p < 1 = |1|_p.$$

Then since $\zeta = b_1 \cdot 1 + (\zeta - b_1)$, by the uniqueness of the p-adic division algorithm, $b_1 = q_1$.

In the inductive case, assume $q_i = b_i$ and $\zeta_i = \frac{\eta_{i-2}}{\eta_{i-1}}$. Then,

$$(\zeta_{i+1})^{-1} = \zeta_i - b_i = \frac{\eta_{i-2}}{\eta_{i-1}} - q_i = \frac{\eta_{i-2} - q_i \eta_{i-1}}{\eta_{i-1}} = \frac{\eta_i}{\eta_{i-1}}.$$

Thus, $\zeta_{i+1} = \frac{\eta_{i-1}}{n_i}$.

Now consider

$$\eta_{i-1} = b_{i+1} \eta_i + (\eta_{i-1} - b_{i+1} \eta_i).$$

Using the same logic from the base case, $|b_{i+1}| < \frac{p}{2}$, and

$$|\eta_{i-1} - b_{i+1} \eta_i|_p = |\eta_i|_p |\zeta_{i+1} - b_{i+1}|_p < |\eta_i|_p.$$

Thus, by the uniqueness of the p-adic division algorithm $b_{i+1} = q_{i+1}$. Therefore, $q_i = b_i$, and by Theorem 4, $\zeta = [q_1, q_2, q_3, \ldots]$. □

Using the theorem in our previous example computes that

$$\frac{\frac{181625}{11}}{\frac{10555}{2}} = 2 + \cfrac{1}{\frac{12}{7} + \cfrac{1}{\frac{-10}{7} + \cfrac{1}{\frac{50}{7^2} + \frac{1}{\frac{2}{7}}}}}.$$

Even though the p-adic Euclidean Algorithm and Browkin's method produce the same results, the p-adic Euclidean Algorithm is computationally quicker since performing the p-adic division algorithm only requires an inversion modulo a prime power. Further Theorem 5 tells us exactly under what conditions the p-adic Euclidean Algorithm terminates.

Corollary. *For $\sigma, \tau \in \mathbb{Q}_p, \tau \neq 0$, the p-adic Euclidean Algorithm terminates in a finite number of steps if and only if $\sigma/\tau \in \mathbb{Q}$.*

5 Open Questions

The following questions concerning the techniques discussed in this paper remain open to the authors.

- How does the sequence $\{\eta_i\}$ from the computation (σ, τ) relate to the sequence $\{\eta_i'\}$ from computing (τ, σ)? Examples quickly show that they are not always related in the simple way the remainders are in the classical case.

- Do we have to use the modular representatives $\left\{\frac{1-p}{2} \ldots \frac{p-1}{2}\right\}$ or would another set of representatives also work? Again, small examples will show that if we choose $\{0, \ldots, p-1\}$ as the set of representatives, the p-adic Euclidean Algorithm applied to two rational numbers may not terminate. In a more general setting, do the representatives depend on the choice of uniformizer for the local field?

- In the classical setting the division algorithm leads to modular arithmetic. Is there a similar theory to come from the p-adic division algorithm?

- Lastly, as is always the case, an analagous theory remains to be worked out in the 2-adics.

Acknowledgements: The author would like to thank Erica Fremstad, another Winona State University student, who also worked on the independent study, Dr. Eric Errthum for his mentorship throughout this project, and the anonymous reviewer for the many helpful comments.

References

[1] Browkin, J. *"Continued Fractions in Local Fields,"* Demonstratio Mathematica, 1978.

[2] Gouvea, F. *"p-adic Numbers: An Introduction,"* Universitext, Springer-Verlag, Berline, 1993.

[3] Koblitz, B. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Springer-Verlag, 1984, 2nd ed.

[4] Rotman, J. *Advanced Modern Algebra*, Prentice Hall, 2002.

[5] Serre, J-P. *A Course in Arithmetic*, Springer, 1973.