Corrections to and Comments on 'Essays in Constructive Mathematics'

page 4, line 19, congruence, not congruences

page 17, line 5.

I no longer think that the proof given here can be said to be "in essence" the proof of Proposition 24 of Euclid's Book VII. His lack of convenient notation makes Euclid's proof difficult to follow in detail. The crucial point, it seems to me, is the Porism to Proposition 2 of the Heath edition, but Euclid makes no direct appeal to it.

The Chinese remainder theorem on page 73, proved from first principles in Essay 3.2, easily implies Proposition 24, because it constructs an inverse of $c \bmod ab$ when inverses of $c \bmod a$ and mod b are given.

page 30, footnote.

Change ρ_{i+1} to ρ_{j+1} and change $j = 0, 1, \ldots, n-1$ to $j = 1, 2, \ldots, n-1$.

page 33, top.

A factorization method was sketched by van der Waerden in some editions of *Moderne Algebra.* It is essentially Kronecker's method, and I found van der Waerden's treatment no more satisfactory than Kronecker's.

page 71, 4 lines up.

"Otherwise, if the first entry is greater ... ", not "If the first entry is greater ... "

page 76. A better proof of the Lemma:

Proof. To say $y + x\sqrt{A} \equiv 0 \bmod [ef, eg + e\sqrt{A}]$ is to say that there are numbers r_1, r_2, ..., r_8 for which

$$(r_1+r_2\sqrt{A})ef+(r_3+r_4\sqrt{A})(eg+e\sqrt{A})+y+x\sqrt{A} = (r_5+r_6\sqrt{A})ef+(r_7+r_8\sqrt{A})(eg+e\sqrt{A}).$$

The coefficient of $\sqrt{A}$ on the left is obviously $x \bmod e$ and the coefficient of $\sqrt{A}$ on the right is $0 \bmod e$. Therefore, $x \equiv 0 \bmod e$. Mod ef the coefficient of $\sqrt{A}$ on the left is $r_3e + r_4eg + x$ and the coefficient of $\sqrt{A}$ on the right is $r_7e + r_8eg$, so

$$r_3e + r_4eg + x \equiv r_7e + r_8eg \bmod ef.$$

Since $g^2 \equiv A \bmod f$, which implies $eg^2 \equiv eA \bmod ef$, multiplication of this congruence by g results in $r_3eg+r_4eA+xg \equiv r_7eg+r_8eA \bmod ef$. Mod ef, the terms on the left side of the equation above without $\sqrt{A}$ are r_3eg+r_4eA+y and the terms on the right without $\sqrt{A}$ are $r_7eg+r_8eA \equiv r_3eg+r_4eA+xg \bmod ef$; therefore, $r_3eg+r_4eA+y \equiv r_3eg+r_4eA+xg \bmod ef$, which implies $y \equiv xg \bmod ef$, as was to be shown.

(The statement "$p+q \equiv p+r \bmod n$ implies $q \equiv r \bmod n$" is valid because when $n \geq 1$ the number np is at least as great as p and the number $np - p$ can be added to both sides of the given congruence to find $np + q \equiv np + r \bmod n$, which implies $q \equiv r \bmod n$; when $n = 0$, the given congruence means $p + q = p + r$ and therefore implies $q = r$.)

Conversely, if $y \equiv xg \bmod ef$ and $x \equiv 0 \bmod e$, say $y + s_1ef = xg + s_2ef$ and $x = qe$, then $y + x\sqrt{A} + s_1ef = xg + x\sqrt{A} + s_2ef = qeg + qe\sqrt{A} + s_2ef = q(eg + e\sqrt{A}) + s_2ef$, which shows that $y + x\sqrt{A} \equiv 0 \bmod [ef, eg + e\sqrt{A}]$.

page 91

When $A = 18$ there is a third cycle containing two modules $[3, \sqrt{18}] \sim [6, \sqrt{18}]$. When $A = 20$ there is a fourth cycle containing the single module $[4, 2 + \sqrt{20}]$.

page 104:

Change last term of displayed equation for $q(\nu)$ from $(\mu^2F + 2\mu G + H)$ to H.

page 104. A better proof of the Proposition is:

Proof. Let $[f, g+\sqrt{A}]$ be a given primitive module in canonical form. Use Lemma 2 to find a module $[F, G+\sqrt{A}]$ in canonical form with $[f, g+\sqrt{A}][F, G+\sqrt{A}] \sim [1]$ and F relatively prime to pf. By Theorem 1 of Essay 3.4, $[f, g+\sqrt{A}][F, G+\sqrt{A}] = [fF, z+\sqrt{A}]$ for some z, and by the Corollary to Proposition 3 of Essay 3.3, this module has the form $[y + x\sqrt{A}]$ where $y^2 > Ax^2$. Therefore $fF = y^2 - Ax^2$. Since $A \equiv 0 \bmod p$ and $fF \not\equiv 0 \bmod p$, it follows that $fF \equiv y^2 \not\equiv 0 \bmod p$. Thus $\chi_p(f) = \chi_p(fF^2) = \chi_p(y^2F) = \chi_p(F)$, as was to be shown.

The proof of the analogous theorem for χ_4 in the case $A \equiv 3 \bmod 4$ follows the same steps, except that one needs to prove that if $fF = y^2 - Ax^2$ and fF is odd then $\chi_4(f) = \chi_4(F)$. This follows easily from the observation that y and x must have opposite parity (because fF is odd) so, mod 4, one of the terms y^2 and $-Ax^2$ is 0 and the other is 1, resulting in $\chi_4(fF) = 1$, from which $\chi_4(f) = \chi_4(F)$ follows.

page 108.

Professor Olaf Neumann points out that Gauss also was pursuing questions of the representability of numbers by given quadratic forms, which is surely true.

page 113, beginning of 2nd full paragraph:

Change "Since $r > 0$ and $\sigma^2 - 4\rho\tau$ is not a square," to "Since neither r nor $\sigma^2 - 4\rho\tau$ is zero (because neither $s^2 - 4rt$ nor $\sigma^2 - 4\rho\tau$ is a square),"

page 121, line 5 up:

First word should be "algebraic" not "allowable".

page 132, footnote:

The Chebotarev article in Russian is not as hard to find as I thought; it is reprinted in his Collected Works in Russian.

page 129, 2nd footnote:
Change the exponent κ in the first line to $n\lambda$ and change κ in the second line to λ.

page 147, line 12 up:
Change "with those of n the rows" to "with those of the n rows"

page 160, line 6:
"decompositions" not "decomposition"

page 171, first note:
After end of 1st line insert: "of finite index in"

page 173, line 11:
After "completes" insert: "one half of"

page 187, line 14 up:
Insert "and" before "the Euclidean".

page 187, line 6 up:
G' not $|G'|$

page 190, first line break of epigraph:
algebrai-schen, not algebrais-chen

page 191, line 7 after the statement of the Theorem:
Change "a strongly" to "an equivalent strongly".

pages 197 and 198:
The parenthetical phrase "(the latter because $\mathrm{tr}(s_{m-1}(S)s_{m-1}(S)h(S)^2) = \mathrm{tr}(I) = m$)" after the display two-thirds of the way down the page should be deleted and replaced with "where n is the number of rows and columns in the given symmetric matrix S because $\mathrm{tr}(s_{m-1}(S)s_{m-1}(S)h(S)^2) = \mathrm{tr}(I) = n$" (not in parenthesis).
In addition, m should be changed to n in five places:

1. The display just referred to should say $s_{m-1}(x)$ is $nx^{m-1} + \cdots$, not $mx^{m-1} + \cdots$.
2. In the following line, "leading coefficient $1/n$", not $1/m$.
3. In the following (displayed) line, g_1/n not g_1/m.
4. In the third line from the bottom, c_{m-2}/n not c_{m-2}/m.
5. In the top line on page 198, $1/n$ not $1/m$.

page 202, line 24
Schwartz succeeded Weierstrass, whose health was failing, in 1892, not after Weierstrass's death in 1897.

page 203, line 3 of 2nd full paragraph:

Insert “to” at end.

page 205:
Reference [9] is reprinted (in Russian) in Chebotarev’s Collected Works.

page 206:
Reference [26] is in volume 20 of Euler’s *Opera,* not volume 21. The connection between this paper of Euler and the formulation of the addition formula given in Essay 4.2 is not at all direct.

page 209:
Add page 190 to the entry “Chebotarev”.
Add page 77 to the entry “Dedekind”.

page 211:
Delete entry “the Euclidean algorithm”.

(Last modified November 13, 2012.)