# An Inductive Approach to Formalizing Notions of Number Theory Proofs

Thomas Marthedal Rasmussen

Informatics and Mathematical Modeling,
Technical University of Denmark, Building 321,
DK-2800 Kgs. Lyngby, Denmark
tmr@imm.dtu.dk

**Abstract.** In certain proofs of theorems of, e.g., number theory and the algebra of finite fields, one-to-one correspondences and the "pairing off" of elements often play an important role. In textbook proofs these concepts are often not made precise but if one wants to develop a rigorous formalization they have to be. We have, using an inductive approach, developed constructs for handling these concepts. We illustrate their usefulness by considering formalizations of Euler-Fermat's and Wilson's Theorems. The formalizations have been mechanized in Isabelle/HOL, making a comparison with other approaches possible.

## 1 Introduction

During the past 20–25 years many parts of mathematics have been formalized and mechanized in various settings and using various systems. Mechanizations as such are thus (in general) no longer seen as achievements by themselves.

But what does it mean that a result[1] has been mechanized? At least it means that there is some computer system in which the result can be formulated and that the system can check (more or less automatically) that the proof is correct. But does it also mean that it is formulated in a language which is similar to that in, say, a textbook and/or that the proof follows the same lines of reasoning and uses the same concepts as the proof in the textbook? This is not always the case. One of the arguments in favor of formalized mathematics[2] is that it helps clarify subtle arguments and this in turn can be helpful for developing new theory. But this use of a formalization gets difficult if the mechanization is too far removed from the textbook proof.

In this paper we will discuss formalizations and mechanizations of some basic theorems of number theory with regard to the above observations. We will more

[1] By "result" we mean both the formulation and the proof of a theorem.

[2] We will here not go into a further discussion of the "usefulness" of formalized mathematics. For an (unbiased) view of this matter we refer to [8] which also contains interesting material on the philosophy and history of formalized mathematics together with many examples of concrete systems.

specifically consider a generalization (often referred to as Euler-Fermat's Theorem) of Fermat's Little Theorem (which is a very basic and important result of number theory) together with a related result known as Wilson's Theorem.

The points we want to make are illustrated in the way we have formalized important parts of the theorems of Euler-Fermat and Wilson. Both use notions of "pairing off" elements of sets in a "one-to-one" manner. We have developed an inductive formalism to handle these concepts, called bijection relations. Once the machinery is in place, this seems to be more intuitive and closer to the original mathematical proofs than the formalizations in, e.g., the Boyer-Moore Theorem Prover. We also believe that this inductive approach can be used when formalizing similar concepts in other contexts and, maybe more importantly, that the use of such "advanced" constructs can be very beneficial in general. An inductive approach, e.g., has proven useful in other areas as well [13, 15].

In the end of the 1970's Boyer and Moore mechanized the Unique Prime Factorization Theorem in their theorem prover [2]. Back then it was considered quite an achievement and one of the most substantial results mechanized. Further mechanizations of number theory in the Boyer-Moore Theorem Prover include: Fermat's Little Theorem (1984) [3], Wilson's Theorem (1985) [18] and Quadratic Reciprocity (1992) [19]. The Unique Prime Factorization Theorem was mechanized in Nuprl [6] in 1986 [9]. Recently, Théry compared mechanizations in Coq [4], HOL [7] and PVS [11] of Fermat's Little Theorem [20]. We have mechanized Euler-Fermat's and Wilson's Theorem in the Higher Order Logic (HOL) of the generic proof assistant Isabelle [12]. The mechanization is included in the latest distribution of Isabelle [10]. Substantial parts of other areas of mathematics have also been formalized in Isabelle/HOL, e.g., set theory [16].

The rest of this paper is organized as follows: In Section 2 we recall some basic facts of number theory and give "textbook" proofs for Euler-Fermat's and Wilson's Theorem. Then, in Section 3, we turn to the question of formalizing these proofs. Some parts do not need much work, in the sense that the mathematical development is formal enough to act (directly) as a basis for mechanization, whereas other parts (the "one-to-one" correspondence and "pairing off") need some additional theory and this is where the inductive approach is utilized. We also consider a formalization of Wilson's Theorem closely following the one of [18], which makes a comparison with our approach interesting. In Section 4 we sketch how we have mechanized the results in Isabelle/HOL and in Section 5 we conclude.

More details on the formalization and mechanization described in this paper are given in [17].

## 2 The Theorems of Fermat and Wilson

This section contains material which can be found in most introductory texts on number theory, e.g., [1, 5].

All results will be formulated based on the integers. To ease the presentation we introduce the following naming conventions: We use $m, n$ for positive integers

and $p, q$ for prime numbers. When referring to sets in the following we mean finite sets of integers.

We assume the reader to be familiar with the notions of congruence (mod $m$) and greatest common divisor of two numbers of which we list some properties below:

**Proposition 1.**

1. *If* $\gcd(a, m) = 1$ *and* $\gcd(b, m) = 1$ *then* $\gcd(ab, m) = 1$
2. *If* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$ *then* $ac \equiv bd \pmod{m}$
3. *If* $\gcd(k, m) = 1$ *and* $ka \equiv kb \pmod{m}$ *then* $a \equiv b \pmod{m}$
4. *If* $\gcd(a, m) = 1$ *then for any* $b$ *there exists a unique* $x$ *such that* $0 \leq x < m$ *and* $ax \equiv b \pmod{m}$

In *4.*, if $b$ is 1, $m$ is a prime $p$ and $0 \leq a < p$, we will denote $x$ (which then always exists) $a^{-1}$ (the dependency on $p$ is left implicit).

Euler's *totient function* is $\phi(m) \mathrel{\widehat{=}} \mid \{n \mid \gcd(n, m) = 1 \wedge 0 \leq n < m\} \mid$. In other words, $\phi(m)$ is the number of non-negative integers less than and relatively prime to $m$. Note, $\phi(p) = p - 1$ when $p$ is prime.

**Definition 1.** *A* reduced set of residues (mod $m$) *is any set of* $\phi(m)$ *numbers mutually non-congruent* (mod $m$) *and relatively prime to* $m$.

The set $\Phi_m \mathrel{\widehat{=}} \{n \mid \gcd(n, m) = 1 \wedge 0 \leq n < m\}$ is the most important example of a reduced residue set. Note that, by definition, $|\Phi_m| = \phi(m)$.

If $a$ is some integer and $B$ is some set of integers then $aB \mathrel{\widehat{=}} \{ab \mid b \in B\}$. By utilizing Proposition 1-3 and the fact that elements of a reduced set of residues are mutually non-congruent we can show:

**Lemma 1.** *Let* $\gcd(a, m) = 1$. *If* $Y$ *is a reduced set of residues* (mod $m$) *then* $aY$ *is a reduced set of residues* (mod $m$).

The following result follows fairly easily too.

**Proposition 2.** *Let* $Y$ *and* $Z$ *be two reduced sets of residues* (mod $m$). *Then the elements of* $Y$ *and* $Z$ *can be put in a unique one-to-one correspondence with respect to congruence* (mod $m$).

**Theorem 1 (Euler-Fermat).** *If* $\gcd(a, m) = 1$ *then*

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

*Proof.* Let $Y$ be a reduced set of residues (mod $m$). By Lemma 1 it follows that $aY$ is a reduced set of residues (mod $m$) too. Using Proposition 2 we have that $Y$ and $aY$ can be paired of uniquely with respect to congruence (mod $m$). Thus (Proposition 1-2),

$$\prod Y \equiv \prod aY \pmod{m} \quad \text{iff} \quad \prod Y \equiv a^{\phi(m)} \prod Y \pmod{m}$$

The Theorem now follows using Proposition 1-3 because $\gcd(\prod Y, m) = 1$ by Proposition 1-1. □

We now turn to Wilson's Theorem for which we need the following lemma.

**Lemma 2.** *If* $0 \leq a < p$ *then* $a^2 \equiv 1 \pmod{p}$ *iff* $a = 1$ *or* $a = p - 1$.

**Theorem 2 (Wilson).**

$$(p-1)! \equiv -1 \pmod{p}$$

*Proof.* Assume $0 < a < p$. Clearly, $a^{-1} \neq 0$, hence $0 < a^{-1} < p$ as well (cf. Proposition 1-4). If $a = a^{-1}$ we know by Lemma 2 that $a = 1$ or $a = p-1$. This means that the set $\Theta_p = \{n \mid 1 < n < p-1\}$ can be divided into $\frac{p-3}{2}$ pairs $(a, a^{-1})$ with $aa^{-1} \equiv 1 \pmod{p}$. By Proposition 1-2 we thus get $\prod \Theta_p \equiv 1 \pmod{p}$, hence $(p-2)! \equiv 1 \pmod{p}$. As $p-1 \equiv -1 \pmod{p}$ we finally have $(p-1)! \equiv -1 \pmod{p}$. This proof assumes $p \geq 5$. Clearly the Theorem holds for $p = 2$ and $p = 3$. □

## 3 Formalization

In this section we revisit the proofs of the previous section and fill the gaps necessary for a rigorous formalization. The "gaps" in the proofs are the notions and reasoning of one-to-one correspondences between residue sets and the "pairing off" in Wilson's theorem. Both can be handled in a general framework by means of inductively defined *bijection relations*.

### 3.1 Bijection Relations

**Definition 2.** *Let* $P \subseteq \mathbb{Z} \times \mathbb{Z}$. *The relation* $\sim_P \subseteq \mathcal{P}(\mathbb{Z}) \times \mathcal{P}(\mathbb{Z})$ *is inductively defined as follows*

$$\frac{}{\emptyset \sim_P \emptyset} \qquad \frac{P(a,b) \quad a \notin A \quad b \notin B \quad A \sim_P B}{(\{a\} \cup A) \sim_P (\{b\} \cup B)}$$

It is straightforward to show that $\sim_P$ is symmetric and transitive if $P$ is. The following result follows easily too.

**Lemma 3.** *Let* $f$ *be an injective function with domain* $A$. *If* $P(a, f(a))$ *for all* $a \in A$ *then* $A \sim_P f(A)$.

**Definition 3.** *Let* $P \subseteq \mathbb{Z} \times \mathbb{Z}$. *The set* $\mathrm{BS}_P \subseteq \mathcal{P}(\mathbb{Z})$ *is inductively defined as follows*

$$\frac{}{\emptyset \in \mathrm{BS}_P} \qquad \frac{P(a,a') \quad a \notin A \quad a' \notin A \quad A \in \mathrm{BS}_P}{(\{a,a'\} \cup A) \in \mathrm{BS}_P}.$$

We now want to relate $\sim_P$ and $\mathrm{BS}_P$ by (roughly speaking) showing that if $A \sim_P A$ then $A \in \mathrm{BS}_P$. For this we first prove the more general result of Proposition 3 below. This only holds, though, if we assume that $P$ is symmetric and satisfies certain uniqueness and totality properties. We will for space limitations not go into the details here and, hence, only sketch the proof below.

**Proposition 3.** *If $A \sim_P B$ then for all $F$, if $F \subseteq A$ and $F \subseteq B$ then $F \in \mathrm{BS}_P$*

*Proof.* (Sketch) Assume $A \sim_P B$, $F \subseteq A$ and $F \subseteq B$ for arbitrary $F$. We must show $F \in \mathrm{BS}_P$ We proceed by induction on the definition of $\sim_P$. The base case ($A = B = \emptyset$) is trivial. Thus, assume $A = \{a\} \cup A'$ and $B = \{b\} \cup B'$ because $P(a, b)$, $a \notin A'$, $b \notin B'$ and $A' \sim_P B'$. By induction we have: For all $G$, if $G \subseteq A'$ and $G \subseteq B'$ then $G \in \mathrm{BS}_P$ $(*)$. Assume $a = b$. We now consider two cases. If $a = b \notin F$ then we are immediately done by $(*)$. If $a = b \in F$ then $(F \backslash \{a\}) \subseteq A'$ and $(F \backslash \{a\}) \subseteq B'$. By $(*)$ we hence get $(F \backslash \{a\}) \in \mathrm{BS}_P$ which finally gives $F \in \mathrm{BS}_P$ by definition of $\mathrm{BS}_P$. Now, assume $a \neq b$. We have four cases depending on whether $a, b$ belongs to $F$. We here only consider $a \in F$ and $b \in F$ in which case $(F \backslash \{a, b\}) \subseteq A'$ and $(F \backslash \{a, b\}) \subseteq B'$. This gives $(F \backslash \{a, b\}) \in \mathrm{BS}_P$ by $(*)$ and then $F \in \mathrm{BS}_P$ by definition of $\mathrm{BS}_P$. □

**Corollary 1.** *If $A \sim_P A$ then $A \in \mathrm{BS}_P$*

### 3.2 Euler-Fermat's Theorem

**Lemma 4.** *Let $Y$ be a reduced set of residues* (mod $m$)*. The function taking $a$ to $a$* mod $m$ *is a bijection from $Y$ to $\Phi_m$.*

Utilizing the Lemmas 3 and 4 we can now show:

**Proposition 4.** *If $Y$ and $Z$ are reduced sets of residues* (mod $m$) *then $Y \sim_{\equiv} Z$*

By simple induction it follows that if $A \sim_{\equiv} B$ then $\prod A \equiv \prod B \pmod{m}$. Thus, by using the inductively defined bijection relations we have made precise what we mean by establishing a one-to-one correspondence between two reduced sets of residues (compare Propositions 2 and 4).

### 3.3 Wilson's Theorem

The "gap" in the proof of Wilson's Theorem (Theorem 2) is the "pairing off" of elements in the set $\Theta_p$. We thus need to formalize this notion so as to prove $\prod \Theta_p \equiv 1 \pmod{p}$ in a more rigorous way. We present two different ways of doing this. The first one (the concrete approach) is based on the work of Russinoff [18]. The second one (the inductive approach) uses bijection relations.

We will below need the following lemma (which can be proved utilizing Lemma 2).

**Lemma 5.** *If $1 < a < p - 1$ then $1 < a^{-1} < p - 1$ and $a^{-1} \neq a$*

**The Concrete Approach** We call this approach "concrete" as it is based on an explicit definition of $a^{-1}$ as follows: $a^{-1} \mathrel{\widehat{=}} a^{p-2} \bmod p$. Clearly, $0 \leq a^{-1} < p$ and using Theorem 1 this definition is thus easily shown correct. By Theorem 1 we can show the following lemma as well.

**Lemma 6.** *If* $0 < a < p$ *then* $(a^{-1})^{-1} = a$

**Definition 4.** $\omega(a) = \textit{if } a > 1 \textit{ then let } v = \omega(a-1) \textit{ in}$
$\textit{if } a \in v \textit{ then } v \textit{ else } \{a\} \cup \{a^{-1}\} \cup v$
$\textit{else } \emptyset$

We are interested in the set $\omega(p-2)$. By induction on the definition of $\omega(a)$ we can show $b \in \omega(p-2)$ iff $1 < b < p-1$ (using Lemma 5). As an immediate consequence we have that $\Theta_p = \omega(p-2)$.

**Proposition 5.** *If* $1 < a < p-1$ *and* $1 < b < p-1$ *then* $b \in \omega(a)$ *iff* $b^{-1} \in \omega(a)$

*Proof. Only if*: By induction on the definition of $\omega(a)$. The base case ($\omega(a) = \emptyset$) is trivial. Assume $b \in \omega(a-1)$ implies $b^{-1} \in \omega(a-1)$. We now have to show that $b \in \omega(a)$ implies $b^{-1} \in \omega(a)$. If $b \in \omega(a-1)$ we are done so assume $b \notin \omega(a-1)$. This means $b = a$ or $b = a^{-1}$. In the first case we are done immediately, in the second case we are done by Lemma 6. *If*: We must show that $b \in \omega(a)$ if $b^{-1} \in \omega(a-1)$. Using again Lemma 6 this reduces to the *only if* case. □

**Proposition 6.** *If* $1 < a < p-1$ *then* $\prod \omega(a) \equiv 1 \pmod{p}$

*Proof.* By induction on the definition of $\omega(a)$. The base case ($\omega(a) = \emptyset$) is true by the convention $\prod \emptyset = 1$. Assume $\prod \omega(a-1) \equiv 1 \pmod{p}$. We must show $\prod \omega(a) \equiv 1 \pmod{p}$. If $a \in \omega(a-1)$ we are done so assume $a \notin \omega(a-1)$. By definition we now get $\prod \{a\} \cup \{a^{-1}\} \cup \omega(a-1) \equiv 1 \pmod{p}$ which again is equivalent to $aa^{-1} \prod \omega(a-1) \equiv 1 \pmod{p}$ if $a \notin (\{a^{-1}\} \cup \omega(a-1))$ and $a^{-1} \notin \omega(a-1)$. Assuming the last two conditions we are done by Proposition 1-2 and definition of $a^{-1}$. That $a \notin (\{a^{-1}\} \cup \omega(a-1))$ follows by assumption and Lemma 5. Finally, $a^{-1} \notin \omega(a-1)$ follows from Proposition 5. □

This proposition thus gives $\prod \omega(p-2) \equiv 1 \pmod{p}$ hence $\prod \Theta_p \equiv 1 \pmod{p}$

**The Inductive Approach** Here we give a proof of Wilson's Theorem using the inductively defined bijection relations. We need to consider the binary relation $R_p$ defined as follows: $R_p(a,b)$ iff $(ab \equiv 1 \pmod{p} \wedge 1 < a < p-1 \wedge 1 < b < p-1)$. The following two lemmas are fairly easily derivable:

**Lemma 7.** *If* $A \in \mathrm{BS}_{R_p}$ *then* $\prod A \equiv 1 \pmod{p}$

**Lemma 8.** *The function taking* $a$ *to* $a^{-1}$ *is a bijection from* $\Theta_p$ *to* $\Theta_p$.

We have $R_p(a, a^{-1})$ for all $a \in \Theta_p$ (cf. Lemma 5). Now, Lemma 3 together with Lemma 8 gives $\Theta_p \sim_{R_p} \Theta_p$. By Corollary 1 we get $\Theta_p \in \mathrm{BS}_{R_p}$, and Lemma 7 then finally gives $\prod \Theta_p \equiv 1 \pmod{p}$. Hence we have formalized the "pairing off" using an approach which is closer to the original proof as we have made explicit what we mean by pairing off the elements of $\Theta_p$: $\Theta_p \in \mathrm{BS}_{R_p}$. Also note that we did not utilize Euler-Fermat's Theorem.

## 4 Mechanization

In this section we give an overview of our mechanization in Isabelle/HOL of Euler-Fermat's and Wilson's Theorems.

Isabelle is a generic proof assistant [12]. Various object logics have been (and can be) formalized by extending Isabelle's meta-logic, which is intuitionistic higher order logic. One of the most well-developed object logics is Isabelle/HOL, formalizing higher order logic. Many substantial results of both mathematics and computer science have been formalized in Isabelle/HOL.

Our mechanization is based on existing theories of integers in Isabelle/HOL developed up to and including the operators mod and div. We thus start our mechanization by defining the basic notions of divides, prime numbers, congruence and Euclid's algorithm (not shown below) for the greatest common divisor:

```
consts
  dvd   :: [int,int] => bool      (infixl 70)
  prime :: int set
  cong  :: [int,int,int] => bool  ("[_ = _]'(mod _')")
  gcd   :: [int,int] => int
defs
  dvd_def     "m dvd n == EX k. n=m*k"
  prime_def   "prime == {p. #1<p & (ALL m. m dvd p --> m=#1 | m=p)}"
  cong_def    "[a = b](mod m) == m dvd (a-b)"
```

Notice how integer numerals are identified by prefixing a `#`. Also note that we introduce a special (more readable) syntax for the congruence relation. Based on these definitions we have proven several basic facts of number theory, including those of Proposition 1.

In both the formalizations of Euler-Fermat's and Wilson's Theorems, finite sets play an important role. In Isabelle/HOL there is a theory developing notions of finite sets. This development is based on inductive definitions of the finiteness of a set, the cardinality of a finite set, etc. We utilize this in our development.

The mechanizations of Euler-Fermat's and Wilson's Theorems closely follow the formalizations described in Section 3. Thus, we had to mechanize the bijection relations as discussed in Section 3.1. Fortunately, it is very easy to define such inductive definitions as those of Definition 2 and Definition 3 in Isabelle/HOL.

There is a general approach for allowing inductive definitions in a logic [14]. This approach can (in principle) be used for any logic in which it is possible to prove the Knaster-Tarski Fixedpoint Theorem. Notice that the logic in question is not extended in any way; the properties of the inductive definitions are proved within the logic, including rules for making inductive proofs over the definitions. This approach has been used in Isabelle/HOL which means that the relation $\sim_P$ can be defined almost verbatim[3] as follows:

[3] In essence, only the syntax differs. In particular, note that `:` and `~:` is Isabelle syntax for $\in$ and $\notin$, respectively.

```
inductive "bijR P"
intrs
  empty  "({},{}) : bijR P"
  insert "[| P a b; a ~: A; b ~: B; (A,B) : bijR P |]
         ==> (insert a A, insert b B) : bijR P"
```

such that `(A,B) : bijR P` expresses $A \sim_P B$. We can similarly give an inductive definition such that `A : bijER P` expresses $A \in \mathrm{BS}_P$.

The mechanization of Euler-Fermat's Theorem follows the formalization of Section 3.2. We end up showing:

```
Goal "[| #0<m; gcd(a,m) = #1 |] ==> [a^phi(m) = #1](mod m)";
```

We have mechanized both the concrete and the inductive formalizations of Section 3.3. In both cases we end up proving:

```
Goal "p:prime ==> [fact(p-#1) = #-1](mod p)";
```

## 5 Conclusion

We have presented a formalization and mechanization (in Isabelle/HOL) of two basic theorems of number theory where we used inductive definitions of so-called bijection relations to establish a generalized framework for reasoning of one-to-one correspondences.

Comparing our inductive approach with existing approaches is most easily done with respect to the formalizations of Wilson's Theorem, as we mechanized both the concrete version of Russinoff and our inductive approach in Isabelle/HOL. We observe that the inductive approach gives a cleaner and more modular presentation closer to the original mathematical proof. When it comes to quantity (number of proof steps) the two developments are comparable but if one ignores the bijection relation part the inductive approach gets noticeably shorter. A reason for doing this is that once the "machinery" for handling the bijection relations is in place it can be used unchanged in other contexts as well. This is in particular the case for our formalization of Euler-Fermat's Theorem in Section 3.2.

## Acknowledgments

The work reported in this paper was carried out while the author was visiting Dr. Lawrence C. Paulson at the Computer Laboratory, University of Cambridge, England. I would like to thank Larry Paulson for valuable comments and suggestions to this work, and for always being willing to discuss Isabelle and formalized mathematics in general. I would also like to thank Morten P. Lindegaard for important comments to parts of this paper. Finally, thanks to Dr. Michael R. Hansen for proofreading drafts of this paper.

## References


1. Alan Baker. *A Concise Introduction to the Theory of Numbers*. Cambridge University Press, 1984.
2. R.S. Boyer and J.S. Moore. *A Computational Logic*. Academic Press, 1979.
3. R.S. Boyer and J.S. Moore. Proof Checking the RSA Public Key Encryption Algorithm. *American Mathematical Monthly*, 91(3):181–189, 1984.
4. The Coq Proof Assistant, 2000. `http://coq.inria.fr`.
5. H. Davenport. *The Higher Arithmetic*. Cambridge University Press, sixth edition, 1992.
6. Robert L. Constable et.al. *Implementing Mathematics with the Nuprl Proof Development System*. Prentice-Hall, 1986.
7. M.J.C. Gordon and T.F. Melham. *Introduction to HOL: A Theorem Proving Enviroment for Higher Order Logic*. Cambridge University Press, 1993.
8. John Harrison. Formalized mathematics. Technical Report 36, Turku Centre for Computer Science (TUCS), 1996.
9. Douglas J. Howe. Implementing Number Theory: An Experiment with Nuprl. In *Automated Deduction, CADE-8*, volume 230 of *Lecture Notes in Computer Science*, pages 404–415. Springer-Verlag, 1986.
10. Isabelle99-2, 2001. `http://www.cl.cam.ac.uk/Research/HVG/Isabelle/dist/`.
11. S. Owre, N. Shankar, and J.M. Rushby. *User Guide for the PVS Specification and Verification, Language and Proof Checker*. SRI International, February 1993.
12. Lawrence C. Paulson. *Isabelle, A Generic Theorem Prover*, volume 828 of *Lecture Notes in Computer Science*. Springer-Verlag, 1994.
13. Lawrence C. Paulson. The Inductive Approach to Verifying Cryptographic Protocols. *Journal of Computer Security*, 6:85–128, 1998.
14. Lawrence C. Paulson. A Fixedpoint Approach to (Co)Inductive and (Co)Datatype Definitions. In G. Plotkin, C. Stirling, and M. Tofte, editors, *Proof, Language, and Interaction: Essays in Honour of Robin Milner*, pages 187–211. MIT Press, 2000.
15. Lawrence C. Paulson. A Simple Formalization and Proof for the Mutilated Chess Board. *Logic Journal of the IGPL*, 2001. In press.
16. Lawrence C. Paulson and Krzysztof Grabczewski. Mechanizing Set Theory. *Journal of Automated Reasoning*, 17:291–323, 1996.
17. Thomas M. Rasmussen. Formalizing Basic Number Theory. Technical Report 502, Computer Laboratory, University of Cambridge, September 2000.
18. David M. Russinoff. An Experiment with the Boyer-Moore Theorem Prover: A Proof of Wilson's Theorem. *Journal of Automated Reasoning*, 1:121–139, 1985.
19. David M. Russinoff. A Mechanical Proof of Quadratic Reciprocity. *Journal of Automated Reasoning*, 8:3–21, 1992.
20. Laurent Théry. *Comparing Coq, HOL, PVS on a simple proof of the RSA Public Key Encryption Algorithm*. INRIA Sophia-Antipolis, March 2000. `http://coq.inria.fr/seminaires/comparaison/`.