CISS451: Cryptography and Computer Security
Final exam (takehome)

TYPESETTING ALIGNED EQUATIONS WITH COMMENTS/JUSTIFICATIONS

Here's an example of typesetting aligned computations (with justifications). Suppose I want to prove $(x + y \cdot z) + (-y) \cdot z) = x$. And I can only use the following:

Let $(R, +, \cdot, 0, 1)$ be a ring.

- The definition of R being a ring, i.e., the ring axioms of R.
- Fact 1: If $x \in R$, then $0 \cdot x = 0$.
- Fact 2: If $x \in R$, then $0 \cdot x = 0 = x \cdot 0$.
- Fact 3: If $x + y = 0$, then $y = -x$.
- Fact 4: $y + x = 0$, then $y = -x$.
- Fact 5: If $x \in R$, then $-(-x) = x$.

The I will show $(x + y \cdot z) + (-y) \cdot z) = x$ like this:

$$
\begin{aligned}
(x + y \cdot z) + (-y) \cdot z &= x + (y \cdot z + (-y) \cdot z) && \text{by the associativity axiom of } + \\
&= x + (y + (-y)) \cdot z && \text{by the distributivity axiom} \\
&= x + 0 \cdot z && \text{by the inverse axiom of } + \\
&= x + 0 && \text{by Fact 2} \\
&= x && \text{by neutrality axiom of } +
\end{aligned}
$$

Take a look at the LaTeX code. The `&` are alignment characters.

Q1. What is the ones digit of the following number

$$1357^{2468^{3579^{4680^{5791^{6802^{7913^{8024^{9135}}}}}}}}$$

A complete proof is required.

Solution

Q2. In this question, you will prove several basic facts about groups.

In the proofs below, you assume use the following: Let $(G, *, e)$ be a ring.

- The definition of G being a group, i.e., the group axioms of R.
- Fact 1: Identity element is unique. In other words let $e, e' \in G$ such that

$$e * x = x = x * e$$
$$e' * x = x = x * e'$$

  for all $x \in G$. Then $e = e'$. (This is proposition 202.2.1 in the notes.)
- Fact 2: Inverse of an element is unique. In other words let $x \in G$. Suppose $y, y' \in G$ such that

$$x * y = e = y * x$$
$$x * y' = e = y' * x$$

  Then $y = y'$. (This is proposition 202.2.2 in the notes.)
- Fact 3: Left cancellation holds. In other words, let $a, x, y \in G$ such that

$$a * x = a * y$$

  then

$$x = y$$

  Likewise, if

$$x * a = y * a$$

  then

$$x = y$$

Do not use any justification other than the axioms and Facts 1-3.

Prove the following

(a) $(x^{-1})^{-1} = x$.

(b) $(x * y)^{-1} = y^{-1} * x^{-1}$.

Solution

Q3. Assume the given facts about groups from Q2. Furthermore define x^n for $n \geq 0$ as follows:

$$x^n = \begin{cases} e & \text{if } n = 0 \\ x & \text{if } n = 1 \\ x^{n-1} * x & \text{if } n > 1 \end{cases}$$

This is from the notes which also contains the definition of x raised to a negative power.

Prove that

$$(x^n)^{-1} = (x^{-1})^n$$

for $n \geq 0$ by induction. (This above is also true when n is negative. But you need to prove the above for negative n.)

Q4. Consider the ring $R = (\mathbb{Z}/2)[X]/n$ where $n = X^2 + 1$.

1. What is $|R|$, the size of R?
2. Factorize $n = X^2 + 1$ in $(\mathbb{Z}/2)[X]$.
3. For each element x of R, write down the multiplicative inverse of x. Is R a field?

Solution

Q5. Can RSA be extended to three primes? In other words let p, q, r be *three* (not two) primes and let $N = pqr$. $\phi(N)$ is the Euler totient of N. Let e, d are integers such that $ed \equiv 1 \pmod{N}$. Let x be an integer. Then

$$(x^e)^d \equiv x \pmod{N} \tag{*}$$

If the above is not true, provide a counter-example. Otherwise prove $(*)$.

SOLUTION

Q6. Let p be a prime. Prove that $\sqrt{p}$ is irrational (i.e., not a fraction) using the well-ordering principle. Note: You must use the well-ordering principle.

(Hint: $\sqrt{2}$ is irrational is proven in discrete 1. That was usually proved using proof by contradiction. Redesign the proof to use WOP. Then generalize the proof to and replace 2 by p.)

Solution

Q7. Let p, q be distinct primes. Prove that if $p \mid a$ and $q \mid a$, then $pq \mid a$. (This was used in the proof of RSA in class.)

You must only use fact in the notes.

1. Definition of divisibility
2. Basic properties of divisibility such as $\pm 1 | a$ for all a and linearity of divisibility.
3. Euclidean property
4. Euclid's lemma
5. Extended Euclidean property
6. Fundamental theorem of arithmetic

Solution