1 Reading assignment

- Read page vii of the Preface of [**I-R**]
- Read Sections 1,2 of Chapter I of [**I-R**]
- Further general reading suggestions:
  - Compare with Pages 1-5 of Hardy and Wrights' *Introduction to the Theory of Numbers* (Fifth Edition, Oxford University Press)
  - Read pages 9-18 of H. Davenport's *The Higher Arithmetic* (Fifth Edition, Cambridge University Press). These are sections 1-3: it 1. The laws of arithmetic 2. Proof by Induction 3. Prime numbers
  - I'm writing a book with William Stein entitled *What is Riemann's Hypothesis?* a draft of which is on the web wstein.org/rh/rh/rh.pdf You're invited to take a look at it and—of course–any comments will be gratefully appreciated.

2 Basic notation

Our notation for the (ring of) integers is $\mathbf{Z} := \{\pm n \mid n = 0, 1, 2, \ldots\}$, and the (fields of) rational, real, and complex numbers we'll denote by $\mathbf{Q}, \mathbf{R}, \mathbf{C}$ respectively. The ring of polynomials in a variable X with coefficients in $\mathbf{C}$ is denoted

$$\mathbf{C}[X] := \{\Sigma_{j=0}^{d} a_i X^i \mid a_i \in \mathbf{C}\},$$

and similarly for polynomials in X with any ring of coefficients.

3 Factorization

The issue is clear: you are given a nonzero number N and the idea is to factor (or as the English say, *factorize*) it, if possible, into numbers of smaller absolute value,

$$N = A \cdot B,$$

with $|A|, |B| < |N|$ or to prove that you can't do it—if you can't. Faced with a nonzero polynomial, say, with real coefficients, $P(X)$, the problem is to try to factor it as a product of polynomials (with real coefficients) of smaller degree, or show that you can't.

This factorization problem for integers is ridiculously difficult, given how easy it is to multiply two numbers together. For example, I recently wanted to factor—for a reason too long to explain—the following 204 digit number[1]: $c204 :=$ 34526903293921580314641092817369674040684481568423967 2 $\sim$
1012992064214519445919256941544565276067662360108749727241555708425276527278687763629 59 $\sim$
51962087273561220060103650687168112461098659687818073890148 6527 and here's the agonizing thing:

[1] it is the only "big" factor of the numerator of the 200-th Bernoulli number; it came up in a problem I was working on.

- I *knew* that it factors[2], and yet:
- I had no idea what its factors are!

In order to find a factorization, I appealed to William Stein, who—in turn—appealed (last March) to the people who are expert in this! It took a while, but last month, the factorization was complete. Here is an excerpt of the announcement that Bill Hart, a member of the group who achieved the factorization, sent to *Number Theory List* <NMBRTHRY@listserv.nodak.edu>:

> We are happy to announce the factorization of the numerator of the 200th Bernoulli number:
>
> $$N = 389 * 691 * 5370056528687 * c204$$
>
> $$c204 = p90 * p115$$
>
> $p90 :=$ 149474329044343594528784250333645983079497454292838248852612270757617 ∼ 561057674257880592603.
>
> $p115 =$ 230988849487852221315416645031371036732923661613619208811597595398791 ∼ 1840431532723141985023484762629703896050377709.
>
> The factorization of the 204-digit composite was made possible with the help of many people:
>
> - William Stein and Barry Mazur challenged us to factor this number
> - Sam Wagstaff maintains a table of factorizations of numerators of Bernoulli numbers at `http://homes.cerias.purdue.edu/~ssw/bernoulli/bnum`. According to this table, the 200th Bernoulli number is the 2nd smallest index with unfactored numerator (the first being the 188th Bernoulli number)
> - Cyril Bouvier tried to factor the c204 by ECM up to 60-digit level, using the TALC cluster at Inria Nancy - Grand Est
> - `yoyo@home` tried to factor the c204 by ECM up to 65-digit level, using the help of many volunteers of the distributed computing platform `http://www.rechenkraft.net/yoyo/`
> - after ECM was unsuccessful, we decided to factor the c204 by GNFS
> - many people at mersenneforum helped for the polynomial selection. The best polynomial was found by Shi Bai, using his implementation of Kleinjung's algorithm in CADO-NFS: `http://www.mersenneforum.org/showthread.php?` $p = 298264\#post298264$
> - the sieving was performed by many volunteers at `NFS@home`, thanks to Greg Childers. See `http://escatter11.fullerton.edu/nfs` for more details of NFS@home. This factorization showed that such a distributed effort might be feasible for a new record GNFS factorization, in particular for the polynomial selection. This was the largest GNFS factorization performed by NFS@home to date, the second largest being $2^{1040} + 1$ at 183.7 digits.

[2] You too, will soon see how one might know such things without actually factoring.

- two independent runs of the filtering and linear algebra were done: one by Greg Childers with msieve (`http://www.boo.net/~jasonp/qs.html`) using a 48-core cluster made available by Bill Hart, one by Emmanuel Thomé and Paul Zimmermann with CADO-NFS (`http://cado-nfs.gforge.inria.fr/`), using the Grid 5000 platform.
- the first linear algebra run to complete was the one with CADO-NFS, thus we decided to stop the other run.

I quote this not expecting that you or I understand the intricacies of this project: factorization of $c204$. Rather, here is the moral I take from this story:

1. - It is relatively easy to *multiply* two numbers. Any computer, for example, can check that $p90 * p115$ is $c204$.
   - It is sometimes quite easy to see that a number is *not* prime,
   - but it can be devilishly difficult to actually factor it.
2. The project of factoring a number that big probably can not be done by mere *brute force* and is not a dull project; rather it involves lots of inspired guessing, elegant choices, and streamlined teamwork.

That this sort of thing happens often for numbers that we encounter of roughly that size is the key to modern encryption. You can take two prime numbers p and q of roughly a hundred digits a piece, multiply them together to get a number $c = p \cdot q$ and then publicize such a number to the entire world, conveying *some information*, but use the information of its factorization to keep private some things that you want to be kept private.

4 Prime numbers, irreducible polynomials

If a number > 1 'doesn't factor' we call it **prime**[3]; if a polynomial of degree > 0 in a polynomial ring doesn't factor, we call it **irreducible** (in that polynomial ring). We are going to use a bit of Math 122 as we go along so we will sometimes use the (basic) vocabulary of ring theory. For us the most important rings are associative, commutative rings with unity. That is we can add and multiply in such a ring A with the usual associative, commutative and distributive rules governing these operations and there is an element $1 \in A$ such that $1 \cdot x = x$ for all $x \in A$.

Some vocabulary:

- An element $u \in A$ is called a **unit** in A if there is an element $v \in A$ such that $u \cdot v = 1$; such an element $v \in A$ is called an *inverse* to u. (There is a unique inverse to any unit; can you give a proof of this?)
- Two elements $a, b \in A$ are called **associate** if $a = ub$ for some unit u of A; equivalently, if $b = va$ for some unit u of A.

[3] I was never able to convince my father that 1 is *not* a prime; it's not.

5 Division with remainder

Here are two basic results. Think of how to prove them.

Proposition 1 *Given integers a, b with $b \neq 0$, [we can try to divide a by b, and thereby show that] there is an equation*

$$a = m \cdot b + r$$

where m and r are integers, and $0 \leq r < |b|$. (Call r the remainder after division of a by b).

Of course, b divides a if and only if the remainder after division of a by b, i.e., r, vanishes.

Proposition 2 *Given polynomials $a(X), b(X) \in \mathbf{R}[X]$ with $b(X)$, [long division of $a(X)$ by $b(X)$ shows that] there is an equation*

$$a(X) = m(X) \cdot b(X) + r(X)$$

where m and r are polynomials in $\mathbf{R}[X]$, and where $0 \leq \text{degree}(r) < \text{degree}(b)$.

Proposition 2 remains true if we replace the coefficient field R by any field k (and for the same reason).

In particular, for example, if $a(X) \in k[X]$ has a root, $\theta \in k$ ("root" means that $a(\theta) = 0$) if we form $b(X) := X - \theta$, then Proposition 2 tells us that $a(X) = m(X) \cdot b(X) + r$ where r is of degree 0, i.e., a constant; evaluating that constant by setting $X \mapsto \theta$ shows that $r = 0$. So, $a(X) = (X - \theta) \cdot m(X)$ where $m(X)$ is a polynomial in $k[X]$ of one less degree than $a(X)$.

6 The "fundamental theorem of algebra"

We won't prove this theorem, but use it as a guide. It says:

Theorem 1 *Every polynomial with complex coefficients of degree > 0 has a complex root.*

In other words, using the discussion above, you see that the monic irreducible polynomials in $\mathbf{C}(X)$ are precisely the linear polynomials, and every monic polynomial $P(X)$ of degree d in $\mathbf{C}(X)$ is a product of d linear monic polynomials:

$$P(X) = \prod_{i=1}^{d} (X - \theta_i).$$

The θ_i—i.e., the *roots* of the polynomial $P(X)$ and also are precisely the *zeroes* of the function $P(X)$. (Why?)

7 Order of vanishing

Of course these θ_i may or may not be distinct, so to emphasize this, we can collect the roots that are equal and write $P(X)$ in another form:

$$(*) \qquad P(X) = \prod_{j=1}^{e} (X - \theta_j)^{d_j}$$

where we let the θ_j run through the *distinct* roots and let d_j denote their multiplicities. One way of describing those d_j's is as *the order of vanishing of the polynomial* $P(X)$ *at the point* $X = \theta_j$ as we would do with any of the analytic functions of Calculus. For example, since

$$\lim_{X \to 0} \frac{\sin(X)}{X^1} = 1 \neq 0, \infty$$

that is, we have that $\sin(X)$ vanishes to order 1 at $X = 0$. Similarly for a polynomial $P(X)$ as above, we let $\mathrm{ord}_{X=\theta} P(X) :=$ that number δ such that

$$(**) \qquad \lim_{X \to 0} \frac{P(X)}{(X - \theta)^{\delta}} \neq 0, \infty$$

and we see easily that if we have a representation of $P(X)$ such as **(*)** above, these orders of vanishing actually *exist*, and moreover, $\mathrm{ord}_{X=\theta_j} P(X) = d_j$ for $j = 1, 2, \ldots, e$. We can write:

$$(***) \qquad P(X) = \prod_{j=1}^{e} (X - \theta_j)^{\mathrm{ord}_{X=\theta_j} P(X)}$$

or— remembering that for any complex number θ the order of vanishing of $P(X)$ at $X = \theta$ vanishes unless θ is one of the roots of $P(X)$; i.e., $\mathrm{ord}_{X=\theta} P(X) = 0$ if $\theta \neq \theta_j$ for some j, we could also write **(***)** as:

$$(***) \qquad P(X) = \prod_{\theta \in \mathbf{C}} (X - \theta)^{\mathrm{ord}_{X=\theta} P(X)}$$

without being scared that there are infinitely many factors here, because all but finitely many of them will be 1.

This argument above, by the way, which makes use of the fundamental theorem of algebra, then proves that the factorization of $P(X)$ into products of (monic) linear factors is unique, up to the order of the factors; that is, it proves the *Unique Factorization theorem* for $\mathbf{C}[X]$. This, as we will soon see is overkill: there is a much much simpler proof of this; and a related proof will also get unique factorization in the ring of integers $\mathbf{Z}$. In any event, even before that proof, we can define the order of vanishing of a nonzero number N at a prime p, by the rule that $\mathrm{ord}_p N = \delta$, where δ is the smallest non-negative number such that p^{δ} divides N and $p^{\delta+1}$ does not divide N. We could even form

$$\prod_{p \text{ prime}} p^{\mathrm{ord}_p(N)},$$

but would we know yet that this product is $|N|$??

8 The (consequence of the) Euclidean Algorithm

Some vocabulary: For this, to keep from very minor extra talk, suppose that a and b are positive numbers.

- A **common divisor** of a and b is an integer that divides both a and b.
- **The greatest common divisor** of a and b, denoted $gcd(a, b)$—and sometimes just (a, b) if there can be no confusion—is, as the name implies, the largest common divisor[4].
- A **Linear Combination** of a and b is an integer of the form $ra + sb$ where $r, s \in \mathbf{Z}$.
- **The Least Linear Combo** of a and b is the smallest positive linear combination of a and b.
- **The Least Common Multiple** of a and b, denoted $lcm(a, b)$, is what you think it is.

Note the evident fact that any common divisor of a and b divides every linear combination of a and b.

The deeper fact, one of the consequences of the Euclidean Algorithm is the following:

Theorem 2 *The greatest common divisor of a and b is the least linear combination of a and b.*

The Euclidean Algorithm (which is one of the exercises for the homework set due next Thursday) is, perhaps, the first famous algorithm in mathematics. It gives a procedure for expressing the greatest common divisor of a and b as a linear combination of those numbers; i.e., for actually finding integers r and s such that

$$gcd(a, b) \;=\; ra \;+\; sb.$$

The "bonus" of this algorithm is that it takes surprisingly few steps to find the r and s for large numbers a and b. (The notion of "step" is pretty clear, given the structure of the algorithm.) So, here's a little contest:

> Find a pair of (at most) four-digit numbers a and b for which the Euclidean Algorithm takes lots of steps!

The winner of the contest is the one who comes up with the most number of steps. No prizes though, just plain old glory.

We will discuss the Euclidean Algorithm somewhat in class. Also we'll include in this discussion the notion of gcd for a, b integers, not only those pairs that are both positive.

[4] Since a and b are not both zero, there is such a "largest" common divisor.

Corollary 3 • *Every common divisor of a and b divides $gcd(a, b)$.*

- *The least linear combination of a and b divides every linear combination of a and b.*

Definition 1 *Two integers a, b are* **relatively prime** *if $gcd(a, b) = 1$. Equivalently (thanks to Theorem 2) they are relatively prime if 1 is a linear combo of a and b; i.e., there are integers r, s such that $1 = ra + sb$.*

The only divisors of a prime number p are 1 and p, so a prime number p has the property that for *any* integer a, either

- $gcd(p, a)$ is either equal to 1 (in which case p is relatively prime to a; and therefore 1 can be expressed as a linear combo of p and a) or
- p divides a

. We will discuss this in class. Moreover, any number that has the above property *is* prime.

9 A fundamental divisibility lemma

Lemma 1 (The fundamental divisibility lemma) *If a prime p divides a product of two integers $a \cdot b$ then it either divides a or b (or both).*

Proof. If p divides a we're done, so assume that p is relatively prime to a, and therefore there are integers r, s such that

$$(*) \quad 1 = rp + sa.$$

Multiply **(*)** by b, to get

$$(*) \quad b = rpb + sab.$$

and since p divides both terms on the RHS it divides b. QED

There's a subtle afterthought that one can (and perhaps should) have about this lemma. Namely, that this property of a number *dividing a product of two integers if and only if it divides one of them* is satsified *only* by prime numbers. So, one might take that proeprty as the defining property. We'll discuss this a bit.

Now let's use Lemma 1.

Theorem 4 *(***Fundamental Theorem of Arithmetic***) Any positive number is expressible in a unique way, except for order of factors, as a product of prime numbers.*

We'll prove this in class.

Corollary 5 *Let N be a positive number. Then*

$$N = \prod_{p \text{ prime}} p^{\mathrm{ord}_p(N)}.$$