Bielefeld, April 28, 1997.

Euclid's Lemma.

Here is a proof which is suitable for presentation to beginners: it does not use greatest common divisors, ideals, or "Bézout's Lemma". It works, *mutatis mutandis*, for any Euclidean ring, but it also works as a story about rectangular arrays of dots.

If p is a prime, we have

$$p \mid ab \quad \Longrightarrow \quad p \mid a \quad \text{or} \quad p \mid b\,.$$

To see this, fix a and take the smallest b such that p divides ab but not b. We claim $b = 1$.

Indeed, $b > p$ is impossible because $ab' = a(b-p)$ would still fill the bill. On the other hand, $1 < b < p$ is impossible because we could write $p = nb + b''$ with $b'' < b$ (in other words, repeatedly subtract ab from ap until only ab'' is left). Since p is prime, $b'' \neq 0$ would be a smaller candidate.

Bielefeld, May 11, 1997.

Euler's Prime.

In $\mathbf{F_p}$ for $p = 641$, we have $-1 = 5 \cdot 2^7$. Taking 4-th powers, we get $1 = 625 \cdot 2^{28} = -16 \cdot 2^{28}$, whence

$$-1 = 2^{32}\,.$$

This demolishes Fermat's dream that the numbers $f_n = 2^{2^n} + 1$ might all be primes.

However, *ein süßer Trost ist ihm geblieben*: for $m > n$, the primes p dividing f_n are different from those dividing f_m, since $2^{2^n} \equiv -1 \pmod p$ implies $2^{2^m} \equiv 1 \pmod p$.

(This is Pólya's proof of the infinitude of primes.)

Bielefeld, May 26, 1997.

Vieta's Pi.

Let $\mathcal{P}_n$ be the regular polygon with n sides, A_n its area, and θ_n the angle of one of its sectors. (Note: "angle" has a purely geometric meaning here.) We have $2A_n = n \sin\theta_n$ and hence

$$\frac{A_{2n}}{A_n} = \frac{2n \sin\theta_{2n}}{n \sin\theta_n} = \frac{1}{\cos\theta_{2n}}\,,$$

because $\sin\theta_n = \sin 2\theta_{2n} = 2\sin\theta_{2n}\cos\theta_{2n}$. Putting $u_n = \cos\theta_n$, and recalling the bisection formula for cosines, we thus get the recursion relations

$$u_{2n} = \sqrt{\frac{1+u_n}{2}}\,, \qquad A_{2n} = \frac{A_n}{u_{2n}}\,,$$

starting with $n = 4$ (i.e. the square), $A_4 = 2$, and $u_4 = 0$.

Bielefeld, May 29, 1997.

Pascal's Triangle.

$C(n,k)$ is the number of paths leading from the vertex to the point $P_{n,k}$ in Pascal's Triangle. Since every such path must pass either through $P_{n-1,k-1}$ or through $P_{n-1,k}$, one immediately gets the formuala $C(n,k) = C(n-1,k-1) + C(n-1,k)$.

What fraction of these paths come "from the left", i.e., through $P_{n-1,k-1}$? The answer is k/n, in other words:

$$\frac{C(n-1,k-1)}{C(n,k)} = \frac{k}{n}\,.$$

To see this, recall that $C(n,k)$ is also the number of "words" of length n composed of k letters L and $n-k$ letters R. Imagine them all written down in a rectangle of width n and height $m = C(n,k)$. Since each row contains k letters L, the rectangle has a total of mk of them. How many are in each column? No column has any more of them as any other: in fact, every column could be taken as the first in a lexicographical recording of the words. Hence each column has exactly mk/n letters L. In particular, mk/n words end with an L, which means that the corresponding path comes through $P_{n-1,k-1}$.

The point of these considerations is that they arrive at the usual multiplicative formula for $C(n.k)$ without "counting orbits" — a technique most students swallow but never really digest.