大阶乘模质数学习笔记

以下参考了这篇博客。

求 $n!\mod{p}(n<p)$，其中 p 为质数，可以在 $\mathcal{O}(\sqrt{n}\log n)$ 的复杂度下完成。

考虑根号分块。定义 $f_{u}(x)=\prod_{i=1}^{u}(x+i)$，设 $v=\lfloor\sqrt{n}\rfloor$，那么显然答案为 $\prod_{i=0}^{v-1}f_{v}(iv)\prod_{i=v^{2}+1}^{n}i$。

已有的办法是先分治求出 $f_{v}(x)$，然后多点求值，这样的复杂度是 $\mathcal{O}(\sqrt{n}\log^{2}n)$。

从另一个角度考虑，如果我们知道了所有的 $f_{v}(0),f_{v}(v),\cdots,f_{v}(v^{2})$，那么这个多项式也就唯一确定了。我们考虑从 $f_{1}(0),f_{1}(v)$ 开始倍增利用拉格朗日插值公式求解 f_{v}。

假设当前我们知道了 $f_{d}(0),f_{d}(v),\cdots,f_{d}(dv)$，注意到 $f_{2d}(x)=f_{d}(x)f_{d}(x+d)$，那么如果我们能求出 $f_{d}((d+1)v),\cdots,f_{d}(2dv)$ 和 $f_{d}(d),f_{d}(d+v),\cdots,f_{d}(d+2dv)$，就很容易求出 $f_{2d}(0),\cdots,f_{2d}(2dv)$。

为了方便，我们把这些多项式看作关于 vx 的多项式，这样一来我们已有的项和要求的项都分别是公差为 1 的等差数列。考虑拉格朗日插值公式 $f_{d}(x)=\sum_{i=0}^{d}\left(f_{d}(i)\prod_{j=0,j\neq i}^{d}\frac{x-j}{i-j}\right)$，不妨设我们要求首项为 m 的数列的第 k 项（从 0 开始），那么有 $$ \begin{aligned} f_{d}(m+k)&=\sum_{i=0}^{d}\left(f_{d}(i)\prod_{j=0,j\neq i}^{d}\frac{m+k-j}{i-j}\right)\\ &=\sum_{i=0}^{d}\left(f_{d}(i)\frac{\prod_{j=0}^{d}m+k-j}{i!(d-i)!(-1)^{d-i}}\cdot\frac{1}{m+k-i}\right)\\ &=\left(\prod_{j=0}^{d}m+k-j\right)\sum_{i=0}^{d}\frac{f_{d}(i)}{i!(d-i)!(-1)^{d-i}}\cdot\frac{1}{m+k-i} \end{aligned} $$ 右边显然是个卷积形式，而左边用一个滑窗就可以解决。我们只需要对 $m=d+1$，$m=dv^{-1}$，$m=dv^{-1}+d+1$ 分别计算即可。

倍增的时候我们还需要从 f_{2d} 转移到 f_{2d+1}，这个可以容易地用 $\mathcal{O}(d)$ 转移，不再赘述。

这样每一步的复杂度就是 $\mathcal{O}(d\log d)$，根据主定理，总复杂度是 $\mathcal{O}(v\log v)=\mathcal{O}(\sqrt{n}\log n)$。

~~当然常数跟多项式逆一样感人，但是肯定比多点求值的两个 $\log$ 加大常数好~~

但是有一个小问题，上式只有在所有的 $m+k-i$ 均不为 0 时才成立（$m=dv^{-1}+d+1,k=d$ 时除外，因为用不到），并且也只有这样才能用滑窗转移（转移时要做除法）。我们证明在本问题中，对于足够大的 p，$m+k-i$ 必然不为 0，注意到显然有 $d\le\frac{v}{2}$。

- $m=d+1$ 时，$2d+1\le v+1=\lfloor\sqrt{n}\rfloor+1<\lfloor\sqrt{p}\rfloor+1\le p$。
- $m=dv^{-1}$ 或 $m=dv^{-1}+d+1$ 时，$m+k-i$ 为 0 相当于存在 $-d\le x\le 2d$ 使得 $dv^{-1}+x\equiv 0\pmod{p}$，即存在 $-2d-1\le x\le d$ 使得 $d\equiv vx\pmod{p}$，显然 $x\ge-2d+1$ 时是不可能的，$x=-2d$ 时要有 $v\equiv -2^{-1}\pmod{p}$，这在 $p>2$ 时是不可能的，$x=-2d-1$ 时，$p=7,v=2,d=1$ 是一组反例，但是在 5×10^{7} 内没有找到其它反例（反正如前所述，这种情况没有用）。

不过如果其它问题中 $m+k-i$ 为 0 了也没有关系。这样相当于我们已有和要求的两个等差数列有部分重合，那么重合的部分直接用原值就可以了。实现起来会稍微麻烦一点点。